| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SC-7** | BOUNDARY PROTECTION | |
| **SC-7.1**  **SC-7.1.1**  **SC-7.1.2**  **SC-7.1.3**  **SC-7.1.4** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the external boundary of the information system;* 2. *the organization defines key internal boundaries of the information system;* 3. *the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system; and* 4. *the information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; enterprise security architecture documentation; other relevant documents or records].  **Interview**: [*select from:* Selected organizational personnel with boundary protection responsibilities].  **Test**: [*select from:* Automated mechanisms implementing boundary protection capability within the information system]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-4, AC-20, CA-3, CM-8, MP-2, PL-2, RA-2  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-7.1.1.1** | | **Examine** security plan, information system design documentation, information system architecture documentation, or other relevant documents; [*reviewing*] for the external boundary of the information system. |
|  | |  |
| **SC-7.1.2.1** | | **Examine** security plan, information system design documentation, information system architecture documentation, or other relevant documents; [*reviewing*] for the key internal boundaries of the information system. |
|  | |  |
| **SC-7.1.3.1** | | **Examine** security plan, information system design documentation, information system architecture documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to monitor and control communications at the external boundary of the information system as identified in SC-7.1.1.1 and at key internal boundaries within the system as identified in SC-7.1.2.1. |
| **SC-7.1.3.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-7.1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-7.1.3.1. |
| **SC-7.1.3.3** | | **Interview** an agreed-upon [*basic*]sample of organizational personnel with boundary protection responsibilities for the information system; conducting [*basic*]discussions for further evidence the measures identified in SC-7.1.3.1 are being employed. |
| **SC-7.1.3.4** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-7.1.3.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |  |
| **SC-7.1.4.1** | | **Examine** organization security architecture documentation; [*reviewing*] for the organization security architecture. |
| **SC-7.1.4.2** | | **Examine** security plan, information system design documentation, information system architecture documentation, or other relevant documents; [*reviewing*] for the boundary protection devices and their configuration settings to be employed to connect the information system to external networks or information systems only through managed interfaces consisting of these devices arranged in accordance with the organizational security architecture identified in SC-7.1.4.1. |
| **SC-7.1.4.3** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the boundary protection devices identified in SC-7.1.4.1; [*reviewing*] for evidence that these devices are configured as identified in SC-7.1.4.1. |
| **SC-7.1.4.4** | | **Test** an agreed-upon [*basic*]sample of the boundary protection devices and their configuration settings identified in SC-7.1.4.1; conducting [*basic*] testing for evidence that these devices are operating as intended. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-7(1)** | BOUNDARY PROTECTION |
| **SC-7(1).1**  **SC-7(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization physically allocates publicly accessible information system components to separate subnetworks with separate, physical network interfaces.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-22, CA-3, RA-2, SC-32  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-7(1).1.1.1** | **Examine** security plan, information system design documentation, information system architecture documentation, or other relevant documents; [*reviewing*] for the publicly accessible information system components, and the measures to be employed to physically allocate these components to separate subnetworks with separate, physical network interfaces. |
| **SC-7(1).1.1.2** | **Examine** an agreed-upon [*basic*] sample of the publicly accessible information system components identified in SC-7(1).1.1.1; [*observing*] for evidence that these publicly accessible information system components are physically allocated to separate subnetworks with separate, physical network interfaces. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-7(2)** | BOUNDARY PROTECTION |
| **SC-7(2).1**  **SC-7(2).1.1**  **SC-7(2).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the mediation necessary for public access to the organization’s internal networks; and* 2. *the information system prevents public access into the organization’s internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing boundary protection; list of mediation vehicles for allowing public access to the organization’s internal networks; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing access controls for public access to the organization’s internal networks]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-4, CA-3, CM-6, RA-2  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-7(2).1.1.1** | **Examine** system and communications protection policy, procedures addressing boundary protection, security plan, or other relevant documents; [*reviewing*] for the mediation necessary for public access to organization’s internal networks. |
|  |  |
| **SC-7(2).1.2.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the boundary protection devices and associated configuration settings to be employed to prevent public access into the organization’s internal networks except as appropriately mediated by managed interfaces employing these devices. |
| **SC-7(2).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon representative sample of the boundary protection devices identified in SC-7(2).1.2.1; [*reviewing*] for evidence that these devices are configured as identified in SC-7(2).1.2.1. |
| **SC-7(2).1.2.3** | **Interview** an agreed-upon [*basic*] sample of organization personnel with boundary protection responsibilities; conducting [*basic*] discussions for further evidence that the boundary protection devices identified in SC-7(2).1.2.1 are being applied to prevent access into the organization’s internal network except as appropriately mediated by managed interfaces employing these devices. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-7(3)** | BOUNDARY PROTECTION |
| **SC-7(3).1**  **SC-7(3).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; communications and network traffic monitoring logs; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-4, AC-17, AC-18, CA-3, RA-2, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-7(3).1.1.1** | **Examine** security plan, information system design documentation, information system architecture documentation, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to limit the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. |
| **SC-7(3).1.1.2** | **Examine** the measures (boundary protection devices) deployed to limit the number of access points to the information system; [*reviewing*] or [*observing*] for evidence that the measures identified in SC-7(3).1.1.1 are being applied. |
| **SC-7(3).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for managing boundary protection devices for the information system; conducting [*basic*] discussions for evidence that the measures identified in SC-7(3).1.1.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-7(4)** | BOUNDARY PROTECTION |
| **SC-7(4).1**  **SC-7(4).1.1**  **SC-7(4).1.2**  **SC-7(4).1.3**  **SC-7(4).1.4**  **SC-7(4).1.5**  **SC-7(4).1.6**  **SC-7(4).1.7** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the frequency for reviewing exceptions to traffic flow policy;* 2. *the organization implements a managed interface for each external telecommunication service;* 3. *the organization establishes a traffic flow policy for each managed interface;* 4. *the organization employs security controls as needed to protect the confidentiality and integrity of the information being transmitted;* 5. *the organization documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;* 6. *the organization reviews exceptions to the traffic flow policy in accordance with the organization-defined frequency; and* 7. *the organization removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing boundary protection; traffic flow policy; information system security architecture; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; records of traffic flow policy exceptions; other relevant documents or records].  **Interview**: [*select from:* Selected organizational personnel with boundary protection responsibilities].  **Test**: [*select from:* Managed interfaces implementing organizational traffic flow policy]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-4, CA-3, RA-2, SC-8, SC-9  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-7(4).1.1.1** | **Examine** system and communications protection policy, traffic flow policy, procedures addressing boundary protection, security plan, or other relevant documents; [*reviewing*] for the frequency for reviewing exceptions to the traffic flow policy. |
|  |  |
| **SC-7(4).1.2.1** | **Examine** security plan, acquisition contracts for telecommunication services, or other relevant documents; [*reviewing*] for all external telecommunication services employed. |
| **SC-7(4).1.2.2** | **Examine** security plan, information system design documentation, information system architecture documentation, or other relevant documents; [*reviewing*] for the boundary protection devices and their configuration settings to be employed as a managed interface for each external telecommunication service identified in SC-7(4).1.2.1. |
| **SC-7(4).1.2.3** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the boundary protection devices identified in SC-7(4).1.2.2; [*reviewing*] for evidence that these devices are configured as identified in SC-7(4).1.2.2. |
|  |  |
| **SC-7(4).1.3.1** | **Examine** information security documentation; [*reviewing*] for a traffic policy for each managed interface identified in SC-7(4).1.2.2. |
|  |  |
| **SC-7(4).1.4.1** | **Examine** system and communications protection policy, procedures addressing boundary protection, security plan, or other relevant documents; [*reviewing*] for the security controls to be employed as needed to protect the confidentiality and integrity of the information being transmitted. |
| **SC-7(4).1.4.2** | **Examine** the security controls employed to protect the confidentiality and integrity of the information being transmitted; [*reviewing*] or [*observing*] for evidence that the security controls identified in SC-7(4).1.4.1 are being employed as needed. |
|  |  |
| **SC-7(4).1.5.1** | **Examine** system and communications protection policy, traffic flow policy, procedures addressing boundary protection, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to document each exception to the traffic flow policy with a supporting mission/business need and duration of that need. |
| **SC-7(4).1.5.2** | **Examine** an agreed-upon [*basic*] sample of traffic flow policy exceptions; [*reviewing*] for evidence that the measures identified in SC-7(4).1.5.1 are being applied. |
|  |  |
| **SC-7(4).1.6.1** | **Examine** system and communications protection policy, traffic flow policy, procedures addressing boundary protection, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to reviews exceptions to the traffic flow policy in accordance with the frequency identified in SC-7(4).1.1.1. |
| **SC-7(4).1.6.2** | **Examine** reviews for an agreed-upon [*basic*] sample of traffic flow policy exceptions; [*reviewing*] for evidence that the measures identified in SC-7(4).1.6.1 are being applied. |
| **SC-7(4).1.6.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for reviewing exceptions to the traffic flow policy; conducting [*basic*] discussions for further evidence that the measures identified in SC-7(4).1.6.1 are being applied. |
|  |  |
| **SC-7(4).1.7.1** | **Examine** system and communications protection policy, traffic flow policy, procedures addressing boundary protection, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to identify and remove traffic flow policy exceptions that are no longer supported by an explicit mission/business need. |
| **SC-7(4).1.7.2** | **Examine** traffic flow policy exceptions identified as no longer supported by an explicit mission/business need; [*reviewing*] for evidence that the measures identified in SC-7(4).1.7.1 are being applied to identify traffic flow policy exceptions that are no longer supported by an explicit mission/business need. |
| **SC-7(4).1.7.3** | **Examine** changes to traffic flow policy configurations resulting from the removal of an agreed-upon [*basic*] sample of traffic flow policy exceptions identified in SC-7(4).1.7.2; [*reviewing*] for evidence that the measures identified in SC-7(4).1.7.1 are being applied to remove the traffic flow policy exceptions that are no longer supported by an explicit mission/business need. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 5** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-7(5)** | BOUNDARY PROTECTION |
| **SC-7(5).1**  **SC-7(5).1.1**  **SC-7(5).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the information system, at managed interfaces, denies network traffic by default; and* 2. *the information system, at managed interfaces, allows network traffic by exception.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Interview**: [*select from:* Selected organizational personnel with boundary protection responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-4, CA-3, CM-6, CM-7, SC-5, SC-32  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-7(5).1.1.1** | **Examine** security plan, information system design documentation, information system architecture documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed, at managed interfaces, to deny network traffic by default. |
| **SC-7(5).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-7(5).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-7(5).1.1.1. |
| **SC-7(5).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-7(5).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **SC-7(5).1.2.1** | **Examine** security plan, information system design documentation, information system architecture documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed, at managed interfaces, to allow network traffic by exception. |
| **SC-7(5).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-7(5).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-7(5).1.2.1. |
| **SC-7(5).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-7(5).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 6** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-7(6)** | BOUNDARY PROTECTION |
| **SC-7(6).1**  **SC-7(6).1.1**  **SC-7(6).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization prevents the unauthorized release of information outside of the information system boundary; or* 2. *the organization prevents any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms supporting the fail-safe boundary protection capability within the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-4, CA-3, CM-6, CM-7, SC-5  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-7(6).1.1.1** | **Examine** system and communications protection policy, procedures addressing boundary protection, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to prevent the unauthorized release of information outside of the information system boundary. |
| **SC-7(6).1.1.2** | **Examine** the measures employed to prevent the unauthorized release of information outside the information system boundary; [*reviewing*] for evidence that the measures identified in SC-7(6).1.1.1 are being applied. |
| **SC-7(6).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with boundary protection responsibilities; [*reviewing*] for further evidence that the measures identified in SC-7(6).1.1.1 are being applied. |
|  |  |
| **SC-7(6).1.2.1** | **Examine** security plan, information system design documentation, information system architecture documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to prevent any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms. |
| **SC-7(6).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-7(6).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-7(6).1.2.1. |
| **SC-7(6).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-7(6).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 7** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-7(7)** | BOUNDARY PROTECTION |
| **SC-7(7).1**  **SC-7(7).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms supporting non-remote connections with the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-4, AC-17, AC-19, AC-20, CA-3  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-7(7).1.1.1** | **Examine** security plan, information system design documentation, information system architecture documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to prevent remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks. |
| **SC-7(7).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-7(7).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-7(7).1.1.1. |
| **SC-7(7).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-7(7).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 8** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-7(8)** | BOUNDARY PROTECTION |
| **SC-7(8).1**  **SC-7(8).1.1**  **SC-7(8).1.2**  **SC-7(8).1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the internal communications traffic to be routed to external networks;* 2. *the organization defines the external networks to which the organization-defined internal communications traffic should be routed; and* 3. *the information system routes organization-defined internal communications traffic to organization-defined external networks through authenticated proxy servers within the managed interfaces of boundary protection devices.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Mechanisms implementing managed interfaces within information system boundary protection devices]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-4, AC-20, CA-3  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-7(8).1.1.1** | **Examine** system and communications protection policy, procedures addressing boundary protection, security plan, or other relevant documents; [*reviewing*] for the internal communications traffic to be routed to external networks. |
|  |  |
| **SC-7(8).1.2.1** | **Examine** system and communications protection policy, procedures addressing boundary protection, security plan, or other relevant documents; [*reviewing*] for the external networks to which the internal communications traffic identified in SC-7(8).1.1.1 should be routed. |
|  |  |
| **SC-7(8).1.3.1** | **Examine** security plan, information system design documentation, information system architecture documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to route internal communications traffic identified in SC-7(8).1.1.1 to external networks identified in SC-7(8).1.2.1 through authenticated proxy servers within the managed interfaces of boundary protection devices. |
| **SC-7(8).1.3.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-7(8).1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-7(8).1.3.1. |
| **SC-7(8).1.3.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-7(8).1.3.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 9** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-7(9)** | BOUNDARY PROTECTION |
| **SC-7(9).1**  **SC-7(9).1.1**  **SC-7(9).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the information system, at managed interfaces, denies network traffic; and* 2. *the information system audits internal users (or malicious code) posing a threat to external information systems.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Mechanisms implementing managed interfaces within information system boundary protection devices]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AU-2, CA-3, SC-5, SI-3, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-7(9).1.1.1** | **Examine** security plan, information system design documentation, information system architecture documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed, at managed interfaces, to deny network traffic. |
| **SC-7(9).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-7(9).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-7(9).1.1.1. |
| **SC-7(9).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-7(9).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **SC-7(9).1.2.1** | **Examine** system and communications protection policy, procedures addressing boundary protection, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the measures (including automated mechanisms and their configuration settings) to be employed to audit internal users (or malicious code) posing a threat to external information systems. |
| **SC-7(9).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in SC-7(9).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-7(9).1.2.1. |
| **SC-7(9).1.2.3** | **Examine** an agreed-upon [*basic*]sample of information system audit records; [*reviewing*] for evidence that the measures identified in SC-7(9).1.2.1 are being applied. |
| **SC-7(9).1.2.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with boundary protection responsibilities; [*reviewing*] for further evidence that the measures identified in SC-7(9).1.2.1 are being applied. |
| **SC-7(9).1.2.5** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-7(9).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |
| **ASSESSMENT – Control Enhancement 10** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-7(10)** | BOUNDARY PROTECTION |
| **SC-7(10).1**  **SC-7(10).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization prevents the unauthorized exfiltration of information across managed interfaces.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms preventing unauthorized exfiltration of information across managed interfaces]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-4, CA-3, CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-7(10).1.1.1** | **Examine** security plan, information system design documentation, information system architecture documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to prevent the unauthorized exfiltration of information across managed interfaces. |
| **SC-7(10).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-7(10).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-7(10).1.1.1. |
| **SC-7(10).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-7(10).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 11** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-7(11)** | BOUNDARY PROTECTION |
| **SC-7(11).1**  **SC-7(11).1.1**  **SC-7(11).1.1a**  **SC-7(11).1.1b** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system checks incoming communications to ensure:*   * *the communications are coming from an authorized source; and* * *the communications are routed to an authorized destination.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-4, CM-6, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-7(11).1.1.1**  **SC-7(11).1.1.1.a**  **SC-7(11).1.1.1.b** | **Examine** security plan, information system design documentation, information system architecture documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to check incoming communications to ensure:   * the communications are coming from an authorized source; and * the communications are routed to an authorized destination. |
| **SC-7(11).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of automated mechanisms identified in SC-7(11).1.1.1.a; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-7(11).1.1.1.a to ensure the communications are coming from an authorized source. |
| **SC-7(11).1.1.3** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-7(11).1.1.1.b; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-7(11).1.1.1.b to ensure the communications are routed to an authorized destination. |
| **SC-7(11).1.1.4** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-7(11).1.1.1.a; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
| **SC-7(11).1.1.5** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-7(11).1.1.1.b; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 12** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-7(12)** | BOUNDARY PROTECTION |
| **SC-7(12).1**  **SC-7(12).1.1**  **SC-7(12).1.1a**  **SC-7(12).1.1b**  **SC-7(12).1.1c** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system implements host-based boundary protection mechanisms for:*   * *servers;* * *workstations; and* * *mobile devices.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing host-based boundary protection capability]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-4, AC-19, CM-6, CM-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-7(12).1.1.1**  **SC-7(12).1.1.1.a**  **SC-7(12).1.1.1.b**  **SC-7(12).1.1.1.c** | **Examine** security plan, information system design documentation, information system architecture documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to implement host-based boundary protection mechanisms for:   * servers; * workstations; and * mobile devices. |
| **SC-7(12).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-7(12).1.1.1.a; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-7(12).1.1.1.a to implement host-based boundary protection mechanisms for servers. |
| **SC-7(12).1.1.3** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-7(12).1.1.1.b; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-7(12).1.1.1.b to implement host-based boundary protection mechanisms for workstations. |
| **SC-7(12).1.1.4** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-7(12).1.1.1.c; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-7(12).1.1.1.c to implement host-based boundary protection mechanisms for mobile devices. |
| **SC-7(12).1.1.5** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-7(12).1.1.1.a; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
| **SC-7(12).1.1.6** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-7(12).1.1.1.b; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
| **SC-7(12).1.1.7** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-7(12).1.1.1.c; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |
| **ASSESSMENT – Control Enhancement 13** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-7(13)** | BOUNDARY PROTECTION |
| **SC-7(13).1**  **SC-7(13).1.1**  **SC-7(13).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the key information security tools, mechanisms, and support components to be isolated from other internal information system components; and* 2. *the organization isolates organization-defined key information security tools, mechanisms, and support components from other internal information system components via physically separate subnets with managed interfaces to other portions of the system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; list of security tools and support components to be isolated from other internal information system components; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: SC-2, SC-3, SC-32  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-7(13).1.1.1** | **Examine** system and communications protection policy, procedures addressing boundary protection, security plan, or other relevant documents; [*reviewing*] for the key information security tools, mechanisms, and support components to be isolated from other internal information system components. |
|  |  |
| **SC-7(13).1.2.1** | **Examine** system and communication protection policy, procedures addressing boundary protection, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to isolate the key information security tools, mechanisms, and support components identified in SC-7(13).1.1.1 from other internal information system components via physically separate subnets with managed interfaces to other portions of the system. |
| **SC-7(13).1.2.2** | **Examine** the measures employed to isolate an agreed-upon [*basic*] sample of the security tools, mechanisms, and support components identified in SC-7(13).1.1.1; [*reviewing*] for evidence that the measures identified in SC-7(13).1.2.1 are being applied to isolate security tools, mechanisms, and support components from other internal information system components via physically separate subnets with managed interfaces to other portions of the system. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 14** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-7(14)** | BOUNDARY PROTECTION |
| **SC-7(14).1**  **SC-7(14).1.1**  **SC-7(14).1.2**  **SC-7(14).1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the managed interfaces where boundary protections are to be implemented;* 2. *the organization defines the measures to protect against unauthorized physical connections across boundary protections implemented at organization-defined managed interfaces; and* 3. *the organization protects against unauthorized physical connections across the boundary protections implemented at organization-defined managed interfaces.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; facility communications and wiring diagram; other relevant documents or records].  **Test**: [*select from:* Physical access capability implementing protections against unauthorized physical connections to the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-4, CA-3, CM-6, SC-20, SC-32  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-7(14).1.1.1** | **Examine** system and communications protection policy, procedures addressing boundary protection, security plan, or other relevant documents; [*reviewing*] for the managed interfaces where boundary protections are to be implemented. |
|  |  |
| **SC-7(14).1.2.1** | **Examine** system and communications protection policy, procedures addressing boundary protection, security plan, or other relevant documents; [*reviewing*] for the measures to protect against unauthorized physical connections across boundary protections implemented at the managed interfaces identified in SC-7(14).1.1.1. |
|  |  |
| **SC-7(14).1.3.1** | **Examine** security plan, information system design documentation, information system architecture documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to protect against unauthorized physical connections across the boundary protections implemented at the managed interfaces identified in SC-7(14).1.1.1. |
| **SC-7(14).1.3.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-7(14).1.3.1.; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-7(14).1.3.1. |
| **SC-7(14).1.3.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-7(14).1.3.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 15** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-7(15)** | BOUNDARY PROTECTION |
| **SC-7(15).1**  **SC-7(15).1.1**  **SC-7(15).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the information system routes all networked, privileged accesses through a dedicated, managed interface for purpose of access control; and* 2. *the information system routes all networked, privileged accesses through a dedicated, managed interface for purpose of auditing.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; audit logs; other relevant documents or records].  **Test**: [*select from:* Mechanisms routing networked, privileged access through dedicated managed interfaces]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-2, AC-3, AC-4, AC-6, AU-2, CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-7(15).1.1.1** | **Examine** security plan, information system design documentation, information system architecture documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to route all networked, privileged accesses through a dedicated, managed interface for purpose of access control. |
| **SC-7(15).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-7(15).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-7(15).1.1.1. |
| **SC-7(15).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-7(15).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **SC-7(15).1.2.1** | **Examine** security plan, information system design documentation, information system architecture documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to route all networked, privileged accesses through a dedicated, managed interface for purpose of auditing. |
| **SC-7(15).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-7(15).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-7(15).1.2.1. |
| **SC-7(15).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-7(15).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 16** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-7(16)** | BOUNDARY PROTECTION |
| **SC-7(16).1**  **SC-7(16).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system prevents discovery of specific system components (or devices) composing a managed interface.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Mechanisms preventing discovery of system components at a managed interface]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: SI-4, CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-7(16).1.1.1** | **Examine** security plan, information system design documentation, information system architecture documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to prevent discovery of specific system components (or devices) composing a managed interface. |
| **SC-7(16).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-7(16).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-7(16).1.1.1. |
| **SC-7(16).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-7(16).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 17** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-7(17)** | BOUNDARY PROTECTION |
| **SC-7(17).1**  **SC-7(17).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs automated mechanisms to enforce strict adherence to protocol format.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system architecture; information system configuration settings and associated documentation; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, CM-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-7(17).1.1.1** | **Examine** security plan, information system design documentation, information system architecture documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to enforce strict adherence to protocol format. |
| **SC-7(17).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-7(17).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-7(17).1.1.1. |
| **SC-7(17).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-7(17).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 18** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-7(18)** | BOUNDARY PROTECTION |
| **SC-7(18).1**  **SC-7(18).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the* *information system fails securely in the event of an operational failure of a boundary protection device.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system architecture; information system configuration settings and associated documentation; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, SC-24  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-7(18).1.1.1** | **Examine** security plan, information system design documentation, information system architecture documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to fail the information system securely in the event of an operational failure of a boundary protection device. |
| **SC-7(18).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-7(18).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-7(18).1.1.1. |
| **SC-7(18).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-7(18).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |