Open Servers VLAN Policy

Policy 907

1 Introduction

1.1 The purpose of this Policy is to define standards for connecting to Appalachian State University's network using the Open_Servers University-wide VLAN.

2 Scope

2.1 This Policy applies to all Appalachian State University employees, contractors, vendors and agents with an Appalachian State University-owned or personally owned computer or workstation used to connect to the Appalachian State University network.

3 Definitions

3.1 Open Servers VLAN

   VLAN available in all network domains that in addition to other special conditions allows access to be established to devices located in it FROM untrusted users. In other words, sessions can be initiated to this device by untrusted users.

3.2 Remote Access

   Any access to Appalachian State University's administrative network through a non-Appalachian State University controlled network, device, or medium.

3.3 Network Domains

   Logical and geographical areas of the University-wide data network.

3.4 Trusted User

   Appalachian State University Staff, Faculty, or Third party contractors who have executed a Third Party Connection Agreement.

3.5 Untrusted Users

   Non-administrative users or Internet users that do not meet the definition of a Trusted User (defined above).

4 Policy and Procedure Statements

4.1 General

4.1.1 This University-wide VLAN was created to provide special access from and to the Internet or untrusted network for non-enterprise departmental or individual computers/servers. This exposure requires minimal firewall and security protection be provided by the network security infrastructure. For this reason, malicious hacking attempts on devices in this VLAN are more liable. If these hacking attempts were successful, the hacked server could be used for malicious or inappropriate purposes. Because of this higher potential, special requirements will be placed on membership to this VLAN.

4.2 Requirements

   1. To certify a server's need and readiness to be placed in the Open_Servers VLAN a procedure of due diligence must first be performed.
2. Servers will not be placed in the Open_Servers VLAN without a full explanation of why these machines cannot perform their mission in other more secure VLANs such as the regular Servers VLAN.

3. If it is determined a server must be placed in the Open_Servers VLAN to perform its University educational or business mission, detailed scrutiny will be made to assure the server meets minimum configurations and host based security. 1.It is Network Infrastructure and Control Systems (NICS) departmental mission and responsibility to operate and secure the University-wide intranet and its connectivity to the Internet. Therefore, NICS will make the final decision on server membership in this VLAN.

4. Once membership has been established in the Open_Servers VLAN the server will continue to be scrutinized using various risk assessment methods (including scanning, virus assessment and hacking techniques – see Risk Assessment Policy). This will be done to help insure the server maintains network security and other requirements.

5. A server will be removed from the Open_Servers VLAN immediately and isolated if found to be vulnerable to hacking or if found to have been hacked.

6. The server’s administrator/college consultant will share in this responsibility and will be ultimately responsible in keeping the server upgraded with the latest security patches and other network security software such as virus filters and scanners.

7. Any user of this device who performs system administration functions (Root Access), must meet the definition of "Trusted User", defined below.

8. Servers that are already in this VLAN will fall under the same scrutiny for maintaining membership. Responsible parties need to be prepared to defend these server’s requirement and readiness to be and stay in this VLAN.

9. If a machine that is already in this VLAN is compromised and subsequently removed, its reinstatement to this VLAN will require a new application and possibly an IP# change.

10. The request procedure for adding a server to the Open_Servers VLAN will be comprehensive. Contact your college computer consultant or ASU Tech Support (phone: 828.262.6266, email tech support) to enter this request. This process will take a minimum of 2-4 workdays to complete.

11. NOTE! Before a device will be considered and finally moved to the Open_Servers VLAN it must first be placed in the regular SERVERS VLAN. This must be done by the server’s administrator/consultant BEFORE the request is made for membership. Contact your college consultant or Tech Support to have this done. While in the Servers VLAN the server can be hardened by the server administrator/consultant and will be scrutinized by Network Infrastructure and Control Systems as part of the certification process prior to moving into Open_Servers.

4.3 Enforcement

4.3.1 Anyone found to have violated this Policy may have their network access privileges temporarily or permanently revoked.

5 Additional References

6 Authority

7 Contact Information

8 Original Effective Date

9 Revision Dates