Secure Network Infrastructure

Best Practice

This document will provide recommendations on the planning, design, placement, configuration and management of core network infrastructure devices.

Draft Date: September 25, 2008

OBJECTIVE

Protection of the network infrastructure at the University of Tennessee is necessary to achieve the university’s mission of teaching, learning, research, and public service. The ability to collect, transmit, store and process information is central to these goals. This document outlines the best practices for creating and managing a network infrastructure that is supportive of the university’s mission.

SCOPE

Individuals Covered

This policy applies to all students, faculty, staff, and others—referred to as “users” throughout this policy—who access, use, or handle the university’s IT resources. "Users" include but are not limited to subcontractors, visitors, visiting scholars, potential students, research associates, grant and contract support personnel, media representatives, guest speakers, and non-university entities or individuals who are granted access.

Resources Covered

This policy applies to all university IT resources, whether individually controlled, shared, stand-alone, or networked. It applies to all computers and communication facilities owned, leased, operated, or provided by the university or otherwise connected to university IT resources. This includes but is not limited to networking devices, personal digital assistants, telephones, wireless devices, personal computers, workstations, mainframes, minicomputers, and any associated peripherals and software, whether used for administration, research, teaching, or other purposes. This policy also applies to all personally owned devices used to store, process, or transmit university information or that are otherwise connected to university IT resources.

COMPLIANCE

At minimum, individual university units (e.g. campuses or institutes, departments, colleges, and divisions) must follow these principles and rules while connected to university IT resources. Each unit is responsible for security on its systems and may apply more stringent security standards than those detailed here, provided these do not conflict with or lower standards or requirements established by the IT security strategy, policies, or best practices.

Any non-compliance with the university’s IT security strategy, policies, or best practices must be reported to the position of authority (POA) or their designee for...
IT at the respective campus/institute or the Information Security Office (ISO). The contact information for both entities, the ISO and the POA, can be found at http://security.tennessee.edu/. Non-compliance can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action. The ISO will work with Human Resources and Student Judicial Affairs to develop and implement appropriate sanctions for non-compliance. Issues that cannot be resolved by the ISO will be directed to the Vice President for Information Technology. Critical non-compliance issues will be directed to the Audit Committee of the Board of Trustees.

**CONVENTIONS USED IN THIS DOCUMENT**

For the purposes of this document, the term Network Infrastructure will refer to the following components:

- Border router
- Hardware firewalls
- Network intrusion detection and prevention systems
- Network switches and routers
- Wireless access points

These components enable the transmission of electronic information into, out of and within the university. When these devices are secure, the university is more able to provide confidentiality, integrity and availability of this information.

This document concerns the following activities as they relate to the security and availability of the components listed above:

- **Planning** – planning for selected infrastructure components
- **Design and Placement** – regarding “how many” and “where” questions
- **Configuration** – targeting the administrative settings that impact operations and security
- **Management** – managing routine operational aspects as well as event monitoring

The intended audience is university technology staff members who are charged with the design and administration of network services.

While it is beyond the scope of this document to detail every single practice involved in the design, configuration, management and security enforcement for these devices, every effort has been made to capture critical recommendations from accepted industry best practices.
INFORMATION AND SYSTEM CLASSIFICATION

University faculty, staff, students, and others need to collect, transmit, store, or process information. Protecting the confidentiality, integrity, and availability of this information is the responsibility of the entire university.

The Information Classification Policy (IT0115) and Computer System Classification Policy (IT0116) formalize this responsibility, define a framework for categorizing information and computer systems according to the perceived risk to the university, and provide methodology for implementing these practices. Refer to those policies for definitions of ownership, responsibilities, system, and information classifications mentioned hereafter.

INFORMATION CLASSIFICATION INDICATORS:

Due to the nature of network infrastructure, a problem with any single component (switch, router, firewall, etc.) could quickly impact most or all other components. Additionally, due to the users’ reliance on the core infrastructure, a service problem with any component can cause serious disruption to operations. In the absence of specific Information or System Classification indicators, it is therefore assumed that the **Best Practice is required for all classification levels**; otherwise, the distinctions will be noted as listed below.

- **Public**: Optional, Recommended, or Required
- **Proprietary**: Recommended or Required
- **Confidential**: Recommended or Required
- **Highly Confidential**: Not permitted to connect to the UT network

SYSTEM CLASSIFICATION INDICATORS:

- **Non-Critical**: Optional, Recommended, or Required
- **Critical**: Recommended or Required
- **Highly Critical**: Required

The only additional distinction to make regarding these indicators:

If a system served by a particular network infrastructure component is classified as **Highly Critical** or the information it serves is considered **Highly Confidential**, the Information Security Office must be contacted regarding the activities addressed herein (Planning, Design, Placement, Configuration and Management).
RECOMMENDATIONS FOR ALL INFRASTRUCTURE COMPONENTS

1. Devices should have their system, security, and environmental event logs sent to a remote server for the dual purposes of log security and centralized log analysis (correlation, de-duplication, etc).
   a. Logs should be monitored, at the minimum, for unauthorized access.
   b. For logs related to authorized/unauthorized access, device modifications, or intrusion attempts, follow industry-specific requirements (PCI, HIPAA, FERPA, GLBA, etc) on how long to keep logs online and offline. In the absence of such requirements, logs should be kept online for at least 3 months and offline for at least 1 year.
   c. Event logs should be sent over a secure, dedicated management network.
   d. An incident response plan should be associated with device alerts that meet a certain threshold. Please refer to the Incident Response Process Best Practice.

2. Secure protocols. Devices should be capable of management by multiple secure access protocols via multiple methods (Command-line, web, etc) for maximum administrative effectiveness and security.
   a. Insecure protocols (e.g. Telnet) should be disabled if technically possible and replaced with secure protocols (e.g. SSH).
   b. If web management is available, SSL is required to protect confidentiality of the traffic and allow the user to authenticate the site.

3. A Change Management procedure (CM) should govern any changes to network devices. This procedure should accommodate network integrity and availability through quick restoration of a previous configuration in the event that a change causes failure or decreased security. Please refer to the Change Management Best Practice for more information. Administrators should:
   a. Implement configuration version control by backing up device configurations to an external system for the dual purposes of configuration change management and configuration security.
   b. Implement software version control for the device firmware and/or operating system.
   c. Capture and track IP addressing information: subnets, critical host IPs, naming conventions (DNS), etc.
   d. Utilize standard configurations (similar devices should be configured similarly).
   e. Adhere to a configuration upgrade procedure that follows the organization’s maintenance-window practices.
   f. Be able to track changes made to devices (who and when).
   g. Create and maintain up-to-date network topology documentation.
h. Consider applying digital signatures or hashes to device configuration backup files if the devices are considered Critical or Highly Critical per the Computer System Classification Policy.

i. Use equivalent non-production systems to test configuration changes (if possible) prior to those changes being applied to the production environment if the systems served by that infrastructure are classified as Critical or Highly Critical or if the information served by those infrastructure components is classified as Confidential or Highly Confidential.

4. Devices should have multiple power supplies, each plugged in to separate power circuits with power conditioning and uninterruptible power supplies if possible.

5. Out-of-band management (OOB). Devices should have a network interface card that can be dedicated to a management network separate from production traffic for the dual purposes of management traffic security and production network performance.

6. Administrators should synchronize all system clocks for event correlation/de-duplication purposes.

7. Administrators should change any of the device’s default passwords, including the default password on the serial port (e.g., for switches and routers), and follow the Password Best Practice for all administrator accounts.

8. If there are no plans to use Simple Network Management Protocol (SNMP), administrators should disable it. If using SNMP, administrators should:
   a. Apply the Password Best Practice to read/write SNMP community strings.
   b. Use SNMP version 3 (SNMPv3) instead of versions 1, 2 or 2.5.
   c. Filter ingress/egress SNMP traffic at the perimeter and limit internal SNMP traffic with ACLs.
   d. Segregate SNMP to a dedicated management network (see b.).
   e. Verify that no “public”/”private” community strings exist by using the tool snmpwalk (see 7.).
   f. If possible, make device MIBs read-only.

9. Management access should be limited to select IP addresses through the use of ACLs.

10. Administrators should harden the device by disabling unneeded services (e.g., finger, identd, etc).
11. Administrators should follow established maintenance and patch management guidelines if the device requires firmware or operating system patching or upgrades. If these patches address security problems, they should be applied as soon as possible after their release (on test systems if possible) and tested before put into production.

12. Device physical security should follow the principle of Least Privilege, in which physical access is granted only to the fewest individuals needed to maintain the infrastructure devices.

13. Network components that are to be decommissioned or transferred must have all storage media securely erased according to the Media Sanitization Best Practice.

14. All availability controls and processes (e.g. redundant hardware, uninterruptible power supplies, backup and restore processes, etc.) must be tested to ensure correct operation in case of a failure. These tests must occur before the system is put into operation and must be repeated regularly. Unless compensating controls are put in place, failed tests must be remediated, then repeated until successful. Refer to the Availability Best Practice for more information.

**BORDER ROUTER WITH ACCESS CONTROL LISTS (ACLS)**

15. Redundant border routers and redundant paths should be used to eliminate a single point of failure for a campus bottleneck.

16. Default ACLs should be used to prevent well-known exploits and protect IP addresses and ports that are known to be vulnerable.

17. Protocols that are typically used for system management (e.g., Remote Desktop, SSH) should be restricted to known external source IP addresses at the border.

18. Timely change management procedures should review, add and delete ACLs on a regular basis since these have a tendency to become stale.

19. Any protocol or type of traffic that is specifically denied by the organization’s security policy should be blocked with the boundary router’s packet filter. This centralizes the implementation of these specific security policies, reduces traffic and logging on the interior firewalls and practices the principle of Defense in Depth, especially if interior firewalls block the same traffic.

20. Recommended ingress ACLs are listed in the table below. This list is based on the National Institute of Standards and Technology (NIST) Guidelines on Firewalls and Firewall Policy (http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf). While the NIST document describes firewall policy, these firewall rules are general enough to be appropriate Access Control Lists on a Border Router.
<table>
<thead>
<tr>
<th>Service Category</th>
<th>Service Name</th>
<th>Ports/Protocol</th>
<th>Always block or recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login services</td>
<td>NetBIOS</td>
<td>139/tcp</td>
<td>Always</td>
</tr>
<tr>
<td></td>
<td></td>
<td>512-514/tcp</td>
<td>Always</td>
</tr>
<tr>
<td>SSH</td>
<td></td>
<td>22/tcp</td>
<td>Default Deny for Critical, Highly Critical systems or systems with Confidential Information. Permit known source IPs.</td>
</tr>
<tr>
<td>Remote Procedure Calls and Network File Systems</td>
<td>portmap/rpcbind</td>
<td>111/tcp and udp</td>
<td>Always</td>
</tr>
<tr>
<td>NFS</td>
<td></td>
<td>2029/tcp and udp</td>
<td>Always</td>
</tr>
<tr>
<td>Lockd</td>
<td></td>
<td>4045/tcp and udp</td>
<td>Always</td>
</tr>
<tr>
<td>File sharing</td>
<td>NetBIOS</td>
<td>135/tcp and udp</td>
<td>Always</td>
</tr>
<tr>
<td></td>
<td></td>
<td>137/udp</td>
<td>Always</td>
</tr>
<tr>
<td></td>
<td></td>
<td>138/udp</td>
<td>Always</td>
</tr>
<tr>
<td></td>
<td></td>
<td>139/tcp</td>
<td>Always</td>
</tr>
<tr>
<td></td>
<td></td>
<td>445/tcp and udp</td>
<td>Always</td>
</tr>
<tr>
<td>Remote UNIX windowing</td>
<td>X Windows</td>
<td>6000-6255/tcp</td>
<td>Always</td>
</tr>
<tr>
<td>Naming services</td>
<td>LDAP</td>
<td>389/tcp and udp</td>
<td>Always</td>
</tr>
<tr>
<td></td>
<td></td>
<td>53/tcp</td>
<td>Always block unless external secondary DNS is receiving transfer</td>
</tr>
<tr>
<td></td>
<td>DNS zone transfers</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS</td>
<td>53/udp</td>
<td>Always block unless target is external DNS server</td>
</tr>
<tr>
<td>“Small services”</td>
<td>Time</td>
<td>37/tcp and udp</td>
<td>Always</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ports below 20/tcp and udp</td>
<td>Always</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Service</td>
<td>Port</td>
<td>Access</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------</td>
<td>--------</td>
<td>----------</td>
</tr>
<tr>
<td>Tftp</td>
<td>69/udp</td>
<td>Always</td>
<td></td>
</tr>
<tr>
<td>Finger</td>
<td>79/tcp</td>
<td>Always</td>
<td></td>
</tr>
<tr>
<td>NNTP</td>
<td>119/tcp</td>
<td>Always</td>
<td></td>
</tr>
<tr>
<td>LPD</td>
<td>515/tcp</td>
<td>Always</td>
<td></td>
</tr>
<tr>
<td>Syslog</td>
<td>514/udp</td>
<td>Always</td>
<td></td>
</tr>
<tr>
<td>SNMP</td>
<td>161-162/tcp and udp</td>
<td>Always</td>
<td></td>
</tr>
<tr>
<td>BGP</td>
<td>179/tcp</td>
<td>Always</td>
<td></td>
</tr>
<tr>
<td>SOCKS</td>
<td>1080/tcp</td>
<td>Always</td>
<td></td>
</tr>
<tr>
<td>ICMP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ingress echo request</td>
<td>N/A</td>
<td>Always</td>
<td></td>
</tr>
<tr>
<td>Egress echo replies</td>
<td>N/A</td>
<td>Always block except for “packet too big” replies</td>
<td></td>
</tr>
<tr>
<td>Time exceeded</td>
<td>N/A</td>
<td>Always block except for “packet too big” replies</td>
<td></td>
</tr>
<tr>
<td>Destination unreachable</td>
<td></td>
<td>Always block except for “packet too big” replies</td>
<td></td>
</tr>
<tr>
<td>Database services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oracle</td>
<td>1521</td>
<td>Default Deny for all but allow known source IPs</td>
<td></td>
</tr>
<tr>
<td>MS SQL</td>
<td>1433/tcp and 1434/udp</td>
<td>Default Deny for all but allow known source IPs</td>
<td></td>
</tr>
<tr>
<td>MySQL</td>
<td>3306/tcp/udp</td>
<td>Default Deny for all but allow known source IPs</td>
<td></td>
</tr>
<tr>
<td>IBM DB2</td>
<td>523/tcp</td>
<td>Default Deny for all but allow known source IPs</td>
<td></td>
</tr>
<tr>
<td>IBM Informix</td>
<td>9088-9089/tcp</td>
<td>Default Deny for all but allow known source IPs</td>
<td></td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>5432/tcp</td>
<td>Default Deny for all but allow known source IPs</td>
<td></td>
</tr>
</tbody>
</table>
FIREWALLS

The requirements for installing host-based firewalls on servers and personal computers are detailed in the Secure Server Best Practice and Desktop and Laptop Best Practice documents. Even in cases where regulatory compliance does not specifically mandate hardware firewall separation, hardware firewalls are recommended to segment systems (servers and personal computing devices) which contain information classified as Proprietary or Confidential from other systems which do not include those types of information.

21. Stateful inspection firewalls should be used over simple packet filters, except in the case of the border router/packet filter whose purpose is to provide basic filtering and ACLs before the other campus firewalls.

22. In general, a firewall should be placed between any two networks with different levels of trust. More formally, administrators should install a firewall if there is a change in the level of system classification or information classification between systems/information. Hardware firewalls should be considered in addition to host-based firewalls in the following scenarios:

a. Centralized change management of firewall rules is required
b. Centralized auditing of firewall rules is required
c. Centralized logging of events is required
d. Defense-in-depth (when combined with host-based controls) is required
e. Control access at the host level due to the existence of legacy software requirements is technically infeasible.

23. Firewall configuration backups should not be stored on the network that is being protected by the firewall. Ideally, firewall backups should be performed by an internal mechanism, such as a tape drive.

24. A matrix of network applications should be maintained to aid firewall administrators in rule-base management. This makes the process of managing rule sets less error prone because the types, versions and vulnerabilities of internal applications are clearly communicated to the firewall administrators.

25. Firewall policies should be audited and verified at least quarterly.

26. The Default Deny principle should be followed with ingress rule design.

a. Deny all traffic by default unless a specific rule allows a type of traffic.
b. Place a comprehensive “deny all” rule at the bottom of the rule set.
c. Follow the Default Deny principle on egress traffic under the following Information Classification conditions:

- Public: Optional
- Proprietary: Recommended
- Confidential: Required
27. The principle of Least Privilege should be followed. Administrators should permit the minimum number of protocols from the minimum number of sources to the minimum number of destinations needed to provide the service.

28. The following general firewall recommendations are from the National Institute of Standards and Technology’s Guidelines on Firewalls and Firewall Policy (http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf). Block Ingress traffic that fits the following characteristics:
   a. Non-authenticated source systems that target the destination address of the firewall itself (either the external or the internal firewall address)
   b. A source address of an IP address that is inside the firewall (including the firewall’s internal IP address)
   c. A source address that is reserved for private networks (RFC 1918)
   d. SNMP traffic
   e. Traffic containing IP Source Routing information
   f. A source or destination of localhost (127.0.0.1) or 0.0.0.0
   g. Traffic containing directed broadcast addresses
   h. Traffic from “Bogon” IP addresses. Bogons are IP addresses that are specially reserved by RFCs or unassigned by IANA and are therefore not allocated by ISPs.

29. Administrators should disallow ICMP Time Exceeded messages on egress to prevent an attacker from mapping the network and determining firewall rules (e.g. with the Firewalk utility).

30. Administrators should block ingress access to TCP/UDP ports 135, 137, 138, 139, 445 and 3389 unless allowed for specific systems. This prevents Windows remote logins and file sharing through the firewall. Administrators should also create ingress & egress filters that prevent IP spoofing.

31. Administrators should consider the following scenarios for implementing a High Availability (HA) configuration with the firewall. Since HA addresses Availability and not Confidentiality or Integrity, only the System Classification breakdown will be considered.

   System Classification indicators:
   - **Non-Critical**: Optional
   - **Critical**: Recommended
   - **Highly Critical**: Required

32. Administrators should use public IP addressing only where needed and implement Network Address Translation (NAT) and Port Addressing Translation (PAT) with external IP mapping & pooling everywhere else.
33. Administrators should use Change Management practices to approve rule-base changes.

34. VPNs must not be used to bypass other firewall policy restrictions.

35. The Drop or Reset actions are preferred over Deny or Reject in cases where the traffic is considered malicious. In cases where the traffic is legitimate, but in error, Deny or Reject is preferred.

**NETWORK INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS)**

This section deals with two kinds of devices: pure Intrusion Detection Systems (IDS), which merely alert and log, and Intrusion Prevention Systems (IPS), which alert, log and block traffic. When the recommendation applies to both types, “IDPS” is used; otherwise, the specific type is indicated.

36. Timely signature updates should be available from the vendor. No more than one week should pass between a vendor’s release of new signatures and the IDPS receiving these new signatures. Then, no more than 1 week should lapse before these new signatures are applied.

37. A Change Management procedure specifically designed for IDPS should be developed and followed with regard to adding new signature updates.

38. The monitored traffic should not exceed the bandwidth of either the IDPS or the switch port / network tap that supplies the IDPS with traffic. When increasing bandwidth on an existing network connection or implementing a new network connection, administrators must first plan capacity to ensure the new IDPS will meet bandwidth requirements.

39. IDPS should be:
   a. capable of assembling fragmented packets for multiple operating system types.
   b. capable of logging to a relational database system.
   c. capable of being pulled into a log collector (eg, database or analyzer).
   d. capable of rule customization and tuning.

40. A Change Management procedure should be developed and followed regarding rule customization and tuning.

41. IDPS systems should have multiple network interface cards, one of which can be made “invisible” to other systems and read-only.

42. Placement of IDPS on a particular network should be based on the Information Classification of data on that network.

   Information Classification indicators:
   - **Public**: Optional
   - **Proprietary**: Recommended
   - **Confidential**: Required
   - **Highly Confidential**: Required
43. Administrators should locate IDPS sensors on any network with possible information leakage. The IDPS can be tuned to monitor and report on outbound information leakage.

44. Administrators should consider more specific NIDS placements:
   a. *Perimeter* – to detect attacks from the most likely, untrusted source.
   b. *DMZ* – to detect attacks coming from the machines most likely to be compromised, the “semi-trusted” network.
   d. *Intranet* – to take advantage of the clustering of similar systems (Eg, payroll, HR, etc) and the natural choke points that their firewalls provide. (Here, NIDS are looking for the “inside” attacker.)

45. Administrators should use caution with sending multiple VLANs to the IDPS. If the switch hardware isn’t capable of sending multiple VLANs to a SPAN port, then the operating system of the IDPS sensor must support 802.1q in order to recognize VLAN ID tags and send each VLAN to its own virtual interface on the system. Separate IDPS instances will then need to listen to the different interfaces.

46. Administrators should use caution with SPAN ports as a method of directing traffic to the IDPS, especially if the switch is directing multiple ports to one SPAN port. The total bandwidth of all the ports being aggregated must not exceed that of the SPAN port. Administrators must also determine whether oversize/undersize packets and packets with CRC errors are important because the switch may not duplicate these on the SPAN port. Latency is also a concern with SPAN ports, but a network tap can overcome these limitations.

47. Administrators should know the systems and types of traffic that each IDPS is monitoring. Administrators should follow the application matrix suggestion in the table listed above.

48. Administrators should disable rules for which there is no corresponding system/application in the network. (In the case of Apache web servers only, disable IIS alerts.) This will save precious IDPS bandwidth.

49. In the case of open source detection systems like Snort, care should be taken to run the IDPS on an operating system that can reconstruct packets in the same fashion as most of the systems monitored by the IDPS.

50. Administrators should not use a hub for IDPS access to traffic. Hubs can introduce latency (half-duplex), have single power supplies and cannot be configured to have a read-only port. Use a SPAN port or a network tap.

51. Administrators should consider using SSL proxies to monitor SSL traffic, especially if industry requirements mandate that such traffic be audited.

52. IDPS sensors should have an interface on a management network that is separate from production traffic. The “listening” interface on the production network should be read-only to prevent the IDPS from being attacked.
53. The IDPS system should itself be patched per the Secure Server Best Practice.

54. Inline Intrusion Prevention is recommended. “Promiscuous” (i.e., not inline) Intrusion Detection is recommended.

55. Active Response intrusion prevention is recommended at the perimeter, between different levels of classification, and between wireless and wired networks.

56. IDPS that are anomaly-based as well as signature-based are preferred.

57. Changes in network design should consider available bandwidth for IDPS.

SWITCHES & ROUTERS

58. Administrators should ensure routers and switches are capable of both device-level (e.g. dual power supplies) and network-level (e.g. meshed architecture) High Availability configurations under the following conditions.

- **System Classification indicators:**
  - **Non-Critical:** Optional
  - **Critical:** Recommended
  - **Highly Critical:** Required

59. Administrators should ensure that switches are capable of providing SPAN ports for the purposes of capturing & analyzing production traffic (e.g., Network Intrusion Detection and Prevention).

60. Administrators should disable:

   a. unneeded management services (finger, identd, http, etc).
   b. unneeded control services (bootp, CDP, TCP/UDP small servers, configuration auto-loading, etc).

61. Administrators should enable logging and designate a syslog server.

62. If remote administration is necessary, administrators should require only SSH access to VTYs and define VTY ACLs.

63. Administrators should make sure switch ports are disabled by default and set to guest/limited VLANs.

64. Administrators should enforce one MAC address per switch port.

65. Administrators should not allow “edge” systems to become gateways, routers or DHCP/BOOTP servers.

66. Administrators should not allow spoofing of IP addresses of external networks.

67. Administrators should duplicate border ACLs on the switches for some relevant subset of the border ACLs.
NETWORK ACCESS CONTROL

The following recommendations deal with the infrastructure’s ability to assess the security posture of “supplicant” devices and deny access based on policy violations. Most of the technology called Network Access Control (NAC) is implemented at the switch level, although there can be other components involved, including a management server which drives the assessment process.

68. The following information should be collected from a device before it can be allowed access to the network:
   a. Authenticated username of the user requesting a connection
   b. System name
   c. All associated IP addresses
   d. All associated MAC addresses, including wireless
   e. Operating system version

69. The following services running on unapproved devices (i.e., not officially managed by UT staff members) must be prevented, by technical means if possible, unless approved by the Position of Authority (POA) for that campus or institute:
   a. Wireless access points, switches, hubs, bridges, or routers
   b. DHCP servers or any device that acts as a DHCP server
   c. DNS servers or any device that acts as a DNS server
   d. Any device that consumes a disproportionate amount of network bandwidth
   e. Any device that acts as an unauthorized network gateway
   f. Any device that transmits unauthorized routing protocols, such as BGP or OSPF
   g. Any device that performs network routing and/or bridging functions
   h. Any device that relies on insecure protocols, such as Telnet or FTP

70. Administrators must be able to terminate a device’s access to the university’s information technology resources if that device or user fails to abide by university policies. Termination may occur without contacting the administrator and/or owner of the violating system. These violations can include but are not limited to:
   a. Failure to comply with Information Technology Security Policies and Best Practices
   b. Bandwidth abuse
   c. Virus, Worm, and/or Trojan infections
   d. Attacks against another system
   e. Attacks against a mission critical system
   f. An active or dormant compromised system
g. Unauthorized device and/or service
h. Stolen IP address
i. Denial of service attacks
j. Unauthorized scanning of ports
k. A device with no patch applied to prevent known exploits
l. No antivirus program initiated
m. A system actively sending spam messages

**WIRELESS ACCESS POINTS**

To understand how risks define the cost of security features, an initial risk assessment should be performed based on the classification of the information and assets that will traverse a wireless network.

71. Administrators should:
   a. gain approval from the POA or his/her designee to install an AP.
   b. work with the POA to notify the ISO before the installation and operation of Wireless Access Points (APs) that will be used in processing or transmitting classified data.
   c. conduct a site survey to measure and establish the coverage for the area.
   d. prior to purchase, ensure that the device supports firmware upgrades so that security patches may be deployed as they become available.
   e. verify that the devices under consideration for purchase support the requirements for protecting each level of Information and System Classification.
   f. register all APs connected to the university’s networks.
   g. collect and store a backup of all software, installation manuals, and procedures required to support the wireless network.
   h. properly install all APs safely out of reach to prevent an attacker who could replace a legitimate safeguarded access point with an unsecured, rogue access point.

72. After installation of a wireless network, administrators should:
   a. perform a follow-up risk assessment to ensure the correct configuration of the wireless devices and the security of the information and assets.
   b. test the AP range boundaries and ensure the extent of coverage serves only those devices requiring access.
   c. make sure that the reset function on the AP is used only when needed, and is only accessible by authorized persons.
   d. physically and logically separate wireless communication from direct access to systems residing on the wired network.
   e. where possible, reduce propagation of radio waves outside the facility through the use of directional antennas.
f. change the default SSID of the AP.
g. disable the broadcast SSID feature so that the client SSID must match that of the AP.
h. ensure that the SSID character string does not use any name that can be associated with the university or the area in which the wireless device is in use.
i. ensure that all devices have strong administrative passwords in accordance with the Password Best Practices.
j. make sure that all unneeded default configurations are changed.
k. disable all nonessential protocols on the wireless device.
l. if the wireless device supports logging, turn it on and review the logs on a regular basis. The logs should be sent to a central log collector.
m. make sure that the APs are turned off during times of disuse.
n. proactively monitor the wireless network on a regular basis by both physical inspection and through the use of wireless detection devices.
o. disable and remove any unauthorized access points connected to the University of Tennessee network.
p. ensure that management traffic destined for a wireless device is on a dedicated and separate subnet.
q. when administering the wireless devices remotely, use a secure mode of transmission such as HTTPS or SSH.

INFORMATION CLASSIFICATION GUIDELINES

Highly Confidential information is not allowed to connect to the UT network and will therefore not be shown in the guidelines below.

73. Transmit restricted information (including account authentication information such as passwords) over encrypted channels from source to destination and never store it in an unencrypted manner.

- **Public**: Required. Authenticating information should always be confidential regardless of the information classification. Consider the widespread practice of password reuse.

- **Proprietary**: Required

- **Confidential**: Required

74. Use standard, well-reviewed, and non-proprietary encryptions methods (e.g., WPA, AES, Triple DES, DES-X, Blowfish, etc.) in encryption protocols.

- **Public**: Required. See above note on password reuse.

- **Proprietary**: Required

- **Confidential**: Required
75. Employ strong and encrypted forms of authentication such as RADIUS, TACACS+, or Kerberos for the wireless network.

- **Public**: Required.
- **Proprietary**: Required
- **Confidential**: Required

76. Ensure system administrators proactively monitor intrusion events and are also notified when an event occurs.

- **Public**: Required
- **Proprietary**: Required
- **Confidential**: Required

77. Provide a means to disconnect users or sessions from the wireless device upon a determined amount of time.

- **Public**: Required
- **Proprietary**: Required
- **Confidential**: Required

78. Perform comprehensive security assessments at regular and random intervals to fully understand and validate the wireless network’s security posture and ensure the network supports the goal of uninterrupted operations.

- **Public**: Required.
- **Proprietary**: Required
- **Confidential**: Required

79. Where technically possible, utilize 802.1x authentication for connecting clients; ensuring strong mutual authentication between the supplicant and the Wireless Access Point occurs before data is transmitted between the two.

- **Public**: Recommended
- **Proprietary**: Recommended
- **Confidential**: Required

80. Before connections are allowed onto a wireless network, ensure that a personal host-based firewall as well as an up-to-date antivirus, and all current operating system patches have been installed (see Network Access Termination above).

- **Public**: Recommended
- **Proprietary**: Recommended
- **Confidential**: Required
81. Use WPA-TKIP as the minimum level of encryption.
   • **Public**: Recommended
   • **Proprietary**: Recommended
   • **Confidential**: Required

82. Implement a procedure for detecting rogue wireless access points, considering the Information Classifications for office environments that deal with the following types of information:
   • **Public**: Recommended
   • **Proprietary**: Recommended
   • **Confidential**: Required

**SYSTEM CLASSIFICATION GUIDELINES**

**Highly Critical** systems are not allowed to connect to the UT network and will therefore not be shown in the guidelines below.

83. Locate and take a complete inventory of any other possible wireless devices on the interior and exterior of buildings to determine any radio frequency interference.
   • **Non-Critical**: Required
   • **Critical**: Required

84. Test the wireless devices’ range boundaries to determine the extent of the wireless coverage.
   • **Non-Critical**: Required
   • **Critical**: Required

85. Test all availability controls and processes (e.g. redundant hardware, uninterruptible power supplies, backup and restore processes, etc.) to ensure function in case of failure. These tests should occur before the system goes production and should be repeated regularly.
   • **Non-Critical**: Required
   • **Critical**: Required

86. Use an external and secured database of user profiles as well as provide a means for local administrator authentication in the event of network connectivity issues to the authentication server.
   • **Non-Critical**: Required
   • **Critical**: Required

87. Fully test and deploy software patches and upgrades in a test environment before deployment into production.
   • **Non-Critical**: Required
   • **Critical**: Required
88. Ensure all hardware provides for a redundant architecture to minimize loss of connectivity.
   - **Non-Critical**: Recommended
   - **Critical**: Required

89. Ensure an acceptable threshold for a number of connecting devices is assessed and maintained to reduce degradation of performance.
   - **Non-Critical**: Recommended
   - **Critical**: Required

90. Implement Quality of Service on the wireless device based upon prioritization of service.
   - **Non-Critical**: Recommended
   - **Critical**: Required

91. Ensure personnel are available to address failures during documented production hours. Pagers and on-call lists must be maintained to ensure reachability. Personnel must make every effort to be available while “on-call.”
   - **Non-Critical**: Recommended
   - **Critical**: Required