IT POLICIES

University-wide Policies

Campus-wide Policies

Departmental Policies

Service-specific Policies

UNIVERSITY DATA MANAGEMENT

INCIDENT RESPONSE

AWARENESS & EDUCATION

RESOURCES

CURRENT INITIATIVES

ABOUT THE UIPO

Search Go

Extending the University Data Network

Policy Status
IT-19 Approved: 19-Sept-2008
Source
Office of the Vice President for Information Technology

Scope

This policy applies to all users of Indiana University information technology resources regardless of affiliation, and irrespective of whether those resources are accessed from on-campus or off-campus locations.

Rationale

Certain network devices such as but not limited to hubs, bridges, switches, routers, firewalls, wireless access points (WAPs), network address translators (NATs), remote access servers (RAS), and virtual private network (VPN) servers, if not deployed and configured correctly, can cause service interruptions and make network problems difficult or impossible to isolate and identify. In addition, if not properly secured, these devices can give unauthorized users access to the university network. The installation of these devices must therefore be managed and coordinated.

University Information Technology Services and regional campus counterparts are responsible for the university's data, video, and voice communications network. This includes designing, deploying, documenting, monitoring, maintaining, supporting, and troubleshooting the physical data, video, and voice networks of the university, as well as the management of the Internet Protocol (IP) address spaces assigned to Indiana University (including public and private addresses).

Policy Statement

Neither individuals nor units are permitted to independently deploy network devices that extend the university network, or secure or isolate parts of the university network, except as approved by University Information Technology Services (UITS) or regional campus counterparts or as stipulated under the provisions of this policy.

Procedures

Remote access services:

Individuals and units are not permitted to independently deploy remote access servers, VPN servers, or dial-in modem services.

Layer-2 devices:

Certain layer-2 devices, such as wired hubs and switches, are very common and pose few problems if deployed prudently; therefore, individuals and units may use layer-2 devices to extend the university network as long as such devices meet university networking standards, are properly and securely managed, and are not used to extend the network beyond the room or cubicle containing the data jack to which the layer-2 device is connected. For example, using a wireless access point, wireless repeater, or a very long cable to provide network connectivity to an adjacent building, another floor, or another room is not acceptable. All layer-2 devices must be deployed securely and in such a manner as to not interfere with the rest of the network.

Layer-3 devices:

Deployment of these services and devices will be managed by and coordinated with UITS or regional campus counterparts. Layer-3 devices include but are not limited to routers, firewalls, VPN servers, NATs, proxy servers, and dial-up servers. The deployment of stand-alone firewalls in front of single servers or workstations, or host-based (software) firewalls is acceptable and encouraged. However, if an individual or unit desires to protect multiple devices behind a firewall, or if an individual or unit desires to deploy a device that conceals the MAC or IP addresses of the hosts behind it, an exception must be requested from either UITS or the regional campus counterpart. It should be noted that, if approved, and if multiple hosts are placed behind a NAT device, a problem with any single host behind that device could result in isolation of all hosts behind the NAT device.

Wireless networks:

Individuals and units may not deploy wireless networks without an exception granted in accordance with policy IT-20 Wireless Networking.

Emergency actions:

UITS engineers, service managers, system administrators, and security and network engineers and regional campus counterparts may temporarily suspend or isolate access to an information technology resource or network device when it reasonably appears necessary to protect the confidentiality, integrity, or availability of the resource or device or data, or to protect other computing resources, devices, or data, or to protect the university from potential harm.

Exceptions to this policy:

Requests for exceptions to this policy should be submitted to netdata@indiana.edu or to the relevant campus helpdesk. UITS and/or regional campus counterparts will review requests on a case-by-case basis as appropriate. Approved exceptions to this policy must comply with university networking

standards. UITS and regional campus counterparts will maintain a record of approved exceptions to this policy.

Consultation:
UITS is available to provide consultation or advice related to this policy and may involve the Information Policy and Information Security offices and/or regional Chief Information Officers (CIOs) and others in consultation.

Regional campuses:
Regional campus Chief Information Officers, in coordination with UITS, are responsible for implementing this policy on regional campuses.

Definitions

Extending the network
is defined as connecting something other than a single end-system to a part of the university network (in most cases a data jack). For these purposes, an end-system is defined as a device (e.g., computer) that has no other network connections, physical or virtual, other than the physical link to the data jack. Devices that extend the network include but are not limited to hubs, bridges, switches, routers, firewalls, WAPs, NATs, RAS, VPN servers, or workstations or servers or devices to provide any of this functionality. Connections of end systems to the network are not considered to be extending the network and are not covered by this policy. Also, connecting to machines on the IU network in such a way that the connecting machine does NOT obtain an IU IP address is not covered by this policy (such as by using the Remote Desktop feature of Microsoft Windows).

IP address spaces
in this context means blocks of IP addresses assigned to Indiana University by Internet addressing authorities.

Layer-2 devices
function at the data link layer of the Open Systems Interconnection Basic Reference Model. Typically these are Ethernet devices such as hubs, switches, repeaters, and WAPs. These devices are often used to provide network connectivity to multiple machines in the same room using a single data jack.

Layer-3 devices
function at the network layer of the Open Systems Interconnection Basic Reference Model. Typically these are IP devices such as firewalls, NATs, and packet-filtering routers that isolate or conceal other devices from the rest of the network.

NAT devices
rewrite the IP header of a packet traversing the device, changing the IP source and/or destination addresses. They also change the layer-2, or MAC address, to that of the NAT device. Often the result is to present multiple devices behind a NAT as if they were a single device.

Private IP addresses
are local network addresses that are not routed to the Internet, so that connections to them from other devices on the Internet are not possible. The most common private IP address blocks are 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as defined by RFC 1918.

Public IP addresses
are local network addresses that are routed to the Internet, so that connections to them from other devices on the Internet are allowed.

Remote access
services are defined as any mechanisms that allow a machine outside of the physical university data network to appear as though it is part of the Indiana University network. Typically this involves creating a link over either the data network or a phone line and assigning an Indiana University IP address to the remote machine.

Sanctions

Failure to comply with Indiana University information technology policies may result in sanctions relating to the individual's use of information technology resources (such as suspension or termination of access, or removal of online material); to the individual's employment (up to and including immediate termination of employment in accordance with applicable university policy); to the individual's studies within the university (such as student discipline in accordance with applicable university policy); civil or criminal liability; or any combination of these.

Related Policies, Laws, and Documents

- IT-20 Wireless Networking
- Is my Ethernet switch compatible with the campus network? (KB doc)
- What switches are recommended for use on the campus network? (KB doc)

Responsible Organization

Office of the Vice President for Information Technology
University Information Policy Office

Policy History

- Approved: September 19, 2008
- Interim: June 26, 2008
- Draft: August 17, 2001
- Revised: December 2007
- Revised: March 2008

top