NCSA Network Security Policy

Document Name: NCSA Network Security Policy
Version: 3.1
Accountable: Alex Withers
Authors: Adam Slagell & Mike Dopheide

Reviewed: Sept 21, 2022
Approved: Dec 16, 2021 by IIB

Introduction

NCSA logically divides its network into several different trust zones. Traffic between these zones is monitored by a Network Intrusion Detection System (NIDS), but traffic within a single zone may not be visible to the NIDS. Therefore, systems within a single zone must be trusted and hence hardened to a similar level.

These zones can vary significantly in how they are trusted: from networks trusted little more than the general Internet to networks that require stringent vetting and auditing. Most networks are public, but some are very isolated and not even routed. The common requirements across **all zones** are simply that systems follow University security policies and that the Security and Networking teams can quickly identify the location and responsible party for all hosts on our networks.

Governance

Policy Application

For the purposes of this document, production systems are defined as any system, to include allocated systems, intended to provide reliable computational and/or data services to a networked constituency. These systems include not only “customer facing” hosts, such as web servers, file servers, login nodes, etc., but also the infrastructure required to support these systems, such as backend database servers, backup and storage systems, authentication servers, etc.

NCSA Internal Infrastructure Board (IIB)

The leaders of ADS (Advanced Digital Services), ITS (Information Technology Services), and Security are responsible for application of this policy. These three groups are the service providers of infrastructure at NCSA and meet regularly to discuss security issues and strategy for providing better services.

Audit

Security is responsible to ensure regular auditing of this policy and automates such audits where possible. However, *responsible* does not always mean executing every audit on their own. This is a group endeavor among all the NCSA service providers and requires coordination and cooperation between ADS, ITS and Security.

Violation

Violations of this policy may result in immediate network disconnection of systems by Security. System owners will have to demonstrate compliance before regaining complete network access. Repeat violators or active attempts to circumvent these policies will be reported to senior management at the NCSA, and could result in more severe prohibitions.

Exceptions Process

For any rule or policy, exceptions may be needed. Security will review requests for exceptions. Decisions will be made by Security after appropriate consultation with the NCSA IIB. Appeals to decisions can be made to the Director's Office.

Policy Maintenance

Security will review this policy annually with the leadership of ADS and ITS to see if changes are needed. It will also be updated as needed for new network environments that are created.

NCSA Network Zones

The following zones and their accompanying policies are described logically as specific addresses are subject to change.

High Performance Datacenter (HPDC) Zone

Definition:

This is the zone (formerly called "Zone 1") for production systems in the data center and consists of most machines in 2020 NPCF. It includes both public and private networks.

Types of Systems:

Systems requiring high availability, physical security and high performance networking are hosted here. This includes not just supercomputers, but core storage, security, networking equipment, and more. These systems are first built in a firewalled subzone until fully vetted by the security team, which is responsible for regular auditing of systems against the security requirements below.

Installation Requirements:

- Until vetted, these machines are firewalled as described in the Installation Subzone.

Informational Requirements:

- Maintain and enforce a list of authorized administrators, and keep records up-to-date so that Security can quickly determine responsible parties for the system. At least one responsible party must be a full-time employee working at the NCSA.

- Provide Security with accounts on the system or a way to quickly get access 24/7 for emergencies.
- Notify Security of any sensitive, confidential or regulated data expected to be on the system.
- An accepted vulnerability and patch management plan must be in place.
- Utilize a recognized NCSA change control process.
- Manage local and privileged account passwords with the NCSA-provided password management solution.

Host Configuration Requirements:

- Disable any unnecessary services and accounts, and enforce with host-based firewalls where possible.
    - Inform Security if the list of services changes.
- Enable host-based brute-force mitigations utilizing the security team's host-based IDS if possible.
- Forward system logs to the security team's log collector.
- Utilize non-local accounts for remote access unless otherwise approved.
- Require two-factor bastions, jump-hosts or VPNs for access to administrative interfaces.
- Routing, traffic forwarding, bridging subnets and other forms of internetwork traffic proxy is prohibited without expressed permission from Security & Networking.

Network Monitoring:

All external links in and out of this zone are monitored by the NIDS. New hosts that appear on this network but have not been vetted may be automatically or manually blocked at the border gateway until investigated and vetted. Network traffic entirely within this zone is unmonitored by the NIDS, but network flows are collected.

Installation Subzone

While new systems are being built and configured in this zone and before they are fully vetted by security, they are firewalled in a subzone.

Host Configuration Requirements:

These systems must:

- Use secure, non-default passwords.
- Be protected by a stateful, network firewall that only accepts connections for approved, secure remote access services.

Advanced Computational Health Enclave

Definition:

The Advanced Computational Health Enclave (ACHE) is a physically and virtually segmented zone used exclusively for processing and storing sensitive data include electronic Protected Health Information (ePHI) and Controlled Unclassified Information (CUI).

Types of Systems:

ACHE is the only approved space for storing and processing ePHI and CUI, and both physical and electronic access is restricted to workforce members with approved access. These systems often have high-availability needs, and hence this zone has a separate UPS backup system. Like the HPDC zone, these systems are first built in a firewalled subzone until fully vetted by the security team, which is responsible for the regular auditing of the systems against the additional security requirements below.

ACHE is a separately monitored zone that inherits all of the requirements of systems in the HPDC, plus additional host configuration requirements.

Installation Requirements:

- Until vetted, these machines are firewalled as described in the Installation Subzone.

Informational Requirements for ePHI:

- The authorized set of administrators must all be workforce members of the NCSA Health Care Component (NHCC), and this group's access must be automated by a process approved by the NCSA HIPAA Liaison.
    - The security operations team is part of this group and must be able to access systems 24/7 in an emergency.
- It is assumed that ePHI, which is high risk data, is on these systems. These are not dual-use systems but are only for work related to health and medicine. The NCSA HIPAA Liaison must be informed of any data from new sources on these systems, especially when personally identifying information is recorded.
- Approved (by the NCSA HIPAA Liaison) vulnerability and patch management procedures must be in place.
- Approved (by the NCSA HIPAA Liaison) change control procedures must be implemented and documented.
- Local and privileged account passwords are managed with the NCSA-provided, two-factor password management solution.

Informational Requirements for CUI:

- The authorized set of administrators must all be workforce members of *the NCSA Staff with ACHE Access*, and this group's access must be automated by a process approved by the NCSA CISO.

    - The security operations team is part of this group and must be able to access systems 24/7 in an emergency.
- It is assumed that CUI, which is high risk data, is on these systems. These are not dual-use systems but are only for work related to research involving CUI. The NCSA CISO must be informed of any data from new sources on these systems, especially when personally identifying information is recorded.
- Approved (by the NCSA CISO) vulnerability and patch management procedures must be in place.
- Approved (by the NCSA CISO) change control procedures must be implemented and documented.
- Local and privileged account passwords are managed with the NCSA-provided, two-factor password management solution.

Host Configuration Requirements:

- All unnecessary services and accounts must be disabled, and enforce with host-based firewalls where possible.
- System logs must be forwarded to the security team's log collector.
- Two-factor authentication is required for remote access. Single-sign-on is limited to 10 million seconds, the lifetime of a short-lived grid certificate.
- Brute-force mitigations will be utilized if a system's access path does not support two-factor.
- User are automatically logged-off after 12 hours of inactivity.
- SSH sessions do not last more than 24 hours.
- Access to administrative interfaces requires two-factor bastions, jump-hosts or VPNs.
- Routing, traffic forwarding, bridging subnets and other forms of internetwork traffic proxy is prohibited without expressed permission from Security & Networking.
- ePHI and CUI are encrypted on storage devices and only accessible to proper customer/data owner.
- Shared, writable file-systems must be securely wiped between jobs from different users or organizations.
- Data transfer endpoints must be whitelisted and scoped to the customer's networks.
- Only encrypted methods of data movement are allowed that also protect the integrity of data in transit.
- Motd and other welcome screens for users or administrators must remind them of the systems's sensitivity, the requirement for laptop encryption, that the system is only for authorized staff and clients, and the University's policies for protected data, including HIPAA and CUI policies.

Network Monitoring:

All external links in and out of this zone are monitored by the NIDS. New hosts that appear on this network that have not been vetted and approved may be automatically or manually blocked at the border gateway until investigated and vetted. Network traffic entirely within this zone is unmonitored by the NIDS, but network flows are collected.

Installation Subzone

While new systems are being built and configured in this zone and before they are fully vetted by security, they are firewalled in a subzone.

Host Configuration Requirements:

These systems must:

- Use secure, non-default passwords.
- Be protected by a stateful, network firewall that only accepts connections for approved, secure remote access services.

Research & Internal Services Zone

Definition:

This zone includes all Raised Access Floor (RAF) space in the NCSA building, as well as a logical zone in the NPCF data center.

Types of Systems:

This zone is for servers supporting R&D projects and internal services at NCSA. The IIB determines which systems are placed in this zone based on space, power, cooling, security and networking considerations together with ADS and Security. Systems in this zone do not have the same baseline service level guarantees as those in the HPDC zone, including security services provided.

Servers, whether supporting internal NCSA services or NCSA projects and their customers, are important, and their compromise can have a significant effect on NCSA productivity and reputation. Whether or not they are even considered production servers, the impact can be significant if the data on the systems is exposed due to privacy considerations, regulatory & legal requirements, or confidentiality agreements. Therefore, certain accountability is still required of all these systems.

Informational Requirements:

Systems or their administrators **must**:

- Label systems in the rack and keep labels up-to-date.
- Maintain and provide the security team with:
    - accounts on the system or a way to quickly get access 24/7 for emergencies
    - purpose of the system and notification of any high risk or confidential data (as defined by UIUC policy).
    - a list of authorized administrators and a responsible full-time NCSA staff person
    - a list of necessary services/ports open
    - a plan for vulnerability and patch management

It is important that changes in the information initially provided to the security team are kept up-to-date, and system owners will need to update this annually. Changes to include high risk or confidential data need to be updated as soon as possible by contacting Security.

Host Configuration Requirements:

Systems or their administrators **must**:

- For production systems, use two-factor authentication for administrative remote access, or request an exemption from Security.
- Disable routing, traffic forwarding, bridging between subnets and other forms of internetwork traffic proxy through the host unless approved by Security & Networking.
- For production hosts, forward system logs to the NSCA syslog collector.

Additional Configuration Recommendations:

Systems or their administrators **should**:

- Enable host-based brute-force mitigations utilizing the security team's host-based IDS if possible.
- Use the NCSA LDAP for authorization and an NCSA centralized authentication service.
- Use host-based firewalls to enforce list of services running.

NCSA Office & Wireless Zone

Definition:

This zone includes all of the office and wireless networks that assign NCSA IP addresses. This includes offices in the NCSA building, NPCF and at least one wireless network, but does not include most RAF space.

Types of Systems:

This zone supports a variety of systems including desktops, laptops, portable devices and research systems. This zone is the most flexible and has the fewest security controls. While firewalled subnets are encouraged by default, the policies that apply broadly to every host are campus and NCSA employee security policies and a requirement to register hosts using an NCSA ID before accessing the network.

Informational & Procedural Requirements:

- System owners must follow all campus and NCSA employee policies regarding software updating, virus scanning, data security, incident reporting, etc.
- New systems must be registered with an NCSA ID to receive an IP address and if different from the NCSA ID, give a point-of-contact for Security.
    - The default network type is firewalled, though users can opt-out
    - Network registration is only for NCSA staff and should not be done for guests. Guest accounts and temporary registrations are available for these use cases.
    - Reregistration is required annually.
- Business Office systems are administered and maintained by ITS, and the corresponding workstations and laptops are on a firewalled network.

Host Configuration Requirements:

- Systems do not bridge or create new NCSA subnets (wired or wireless) without approval from Networking & Security.

Network Configuration Requirements for NCSA wireless networks:

The NCSA wireless networks (those giving public NCSA IP addresses) must not give an adversary advantages they wouldn't already have with NCSA authentication credentials and thus could execute from anywhere with VPN access.

- Cryptographic and security configurations will be consistent with UIUC policies and standards of practice.
- These networks authenticate and authorize against the NCSA LDAP service, and are not used for guest access
- Like the default office subnets, the primary wireless network is firewalled or equivalently controlled to not allow servers for outside the NCSA IP space.
- The security team must have the ability to readily map wireless IPs and timestamps to users for at least 90 days.
- Only the NCSA and/or CITES networking teams have the ability and authority to configure access points and networking hardware for the wireless networks NCSA buildings.

VPN Zone

Definition

NCSA offers a VPN services with different authentication profiles. These can be used as more flexible bastions in conjunction with firewall rules, to access privately addressed subnets, or to reach other services that might be blocked at the border (e.g., mounting filesystems).

Security Requirements

Systems connected to the NCSA VPN are monitored unencrypted on the internal side of the VPN with the NIDS. Authentication to the VPN requires the use of valid and authorized NCSA credentials.

Physical Security Zone

Definition:

This is an isolated zone only for the NPCF physical security systems.

Types of Systems:

All NPCF physical security systems, and only those systems, are part of this zone. This includes the camera DVRs, badge readers, iris scanners, ACMS workstations (for badging, control and enrollment), and the ACMS database server.

Host Configuration Requirements:

- Devices on this network can neither connect to the other networks or be connected to except for a single ACMS workstation that must connect with iCard systems elsewhere on campus.
    - This ACMS workstation can only be connected to via RDP from a single remote workstation run by Facilities & Services for troubleshooting and support.
- All other remote connections, even if temporary for support, must be approved by the Security Office.

Isolated Zones

Definition:

Sometimes there is a need for a special subnet that is treated no differently than an external network and does not route internally with NCSA systems. This could be because the systems on the subnet would not meet the requirements of this policy (e.g., they bring their own unmonitored WAN links or cannot be hardened sufficiently), it is actually an external network extruding into our physical infrastructure, or that external requirements or regulations require extra isolation.

Network Configuration Requirements:

- Connections to other NCSA hosts would not be allowed unless exiting and reentering the NCSA network.
    - Security can approve limited exceptions to whitelist direct access to key NCSA services, such as DNS, and these exceptions will be documented.
- Systems in an isolated zone are treated as external from a security perspective. As such, they may not benefit from any of the security services or monitoring normally provided.