

Network Infrastructure Access Control

INTRODUCTION

The purpose of this policy is to define the use of Firewall and other data communication access control mechanisms within the UNMC environment. This policy applies to all systems connected to UNMC network infrastructure and all systems attempting to electronically communicate with UNMC/NHS/UMA systems.

BASIS FOR POLICY

UNMC/NHS/UMA strives to maintain an environment of quality patient care, research, and education. In order to maintain this environment, steps must be taken to ensure that access to important information on computing systems are not compromised, interrupted, or the performance is impaired.

DEFINITIONS

Network Access Control List (ACL) A Network ACL or Network Access Control List is a mechanism on a packet filtering router that can be used to directionally control communication on an interface on the router.

Virtual Private Network (VPN) A VPN or Virtual Private Network refers to an encrypted communication tunnel through a public network. Since all data passing through the tunnel is encrypted, it is referred to as being virtually private.

Firewall A firewall is a network device that is used to control communication services and protocols both to and from different devices.

Network Access Control mechanism would include but not be limited to firewalls, routers, etc.

POLICY

A. Selection

All network access control mechanisms will be selected and implemented by the UNMC network team. Departments and business units will not be allowed to implement access control mechanisms at the network level. ([Link to network equipment policy.](#))

B. Default Configuration

All access control mechanisms will be configured to deny all communication except for the services and protocols that are identified to meet the business and academic needs of the workforce.

C. Request for Access

Before communication through an access control mechanism is allowed, the business need must be submitted to the UNMC network team. (dnsadmin@unmc.edu) In order to expedite the review process, the request should include the following information:

1. All necessary communication protocols and services
2. Source and destination systems
3. Direction of communication
4. Reason for the communication

The UNMC security team will review the request and determine if a security risk would be introduced to the network. If a security risk is identified, the UNMC security team will jointly work with the requestor to identify alternatives to meeting the business or academic need.

D. Implementation Timeframe / Changes

Unless there is a serious business need to implement an access control change quickly, the UNMC network team will complete requests within seven (7) business days. Urgent requests should be identified as such and will be expedited.

E. Bypass

Access control systems must not be bypassed, e.g. peer to peer applications, proxy servers, etc.

F. Placement

Access control mechanisms will be placed between the UNMC trusted network and any untrusted network. Untrusted networks include the public Internet and any network that is not managed by the UNMC network team.

G. Change Control

The UNMC network team will maintain a log of all changes to access control mechanisms for documentation purposes. Log entries will contain the following information.

Date	Time
Access Control Mechanism	Reason for modification
Name of individual making request	Engineer who made the change