CI Network Architecture & Security Standard

Executive Summary

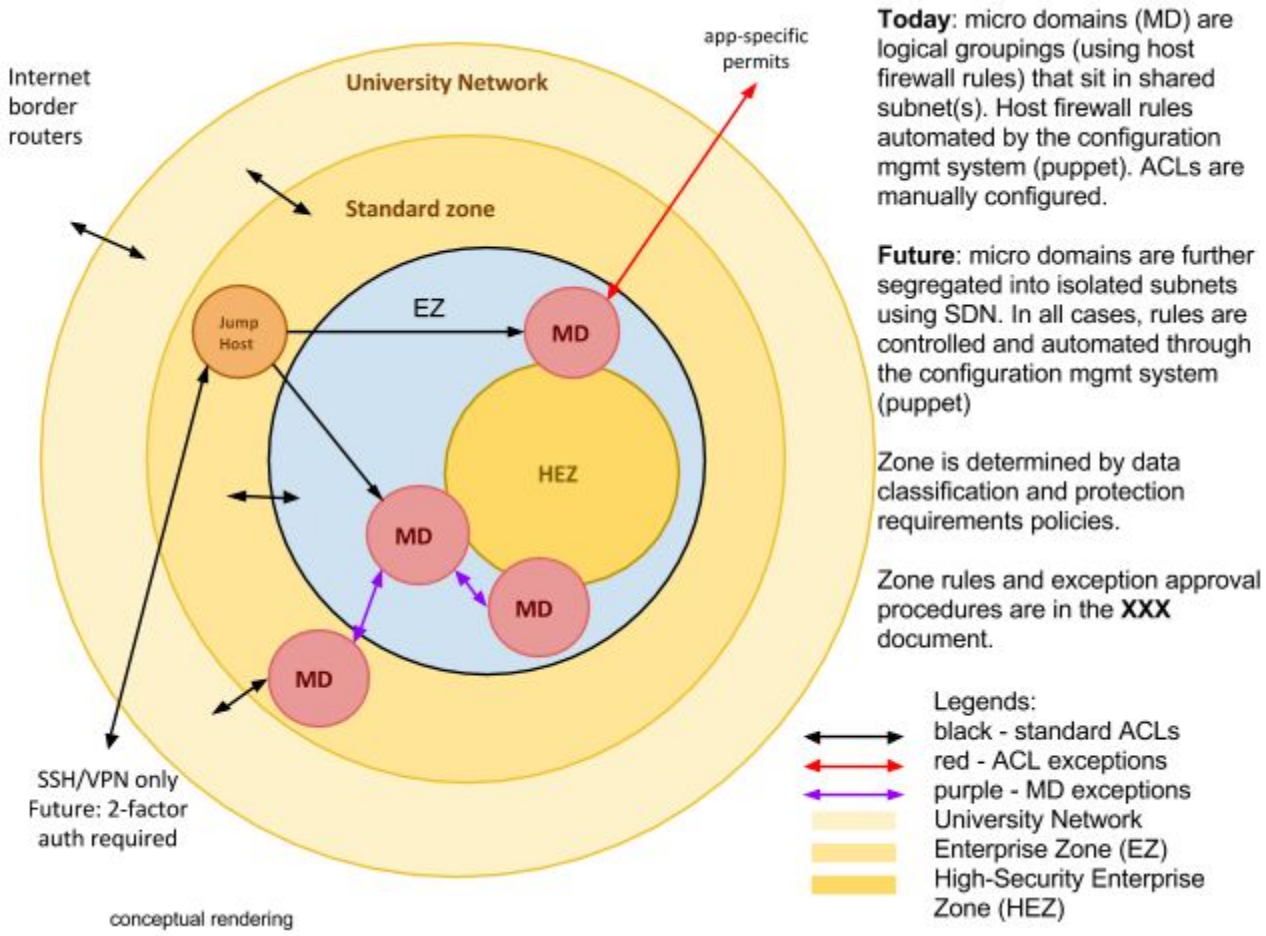
This document represents the current and future standards that will be applied to that infrastructure to provide layered security in the CI environment. It is being designed to provide maximum security to our most sensitive data using an approach that will minimize the approvals and manual processes needed to achieve that goal.

Scope

The scope of this document will cover the current and future network security standards and procedures that will be applied to all servers owned and managed by CUIT in the data centers and cloud IaaS managed by CUIT. It will not be applied to servers residing in CUIT data centers that are not managed by CUIT.

Objectives

1. Reduce number and complexity of Enterprise Zone ACL requests/changes required for CI application deployment, to minimize opportunity for error and reduce manual effort.
2. Eliminate need for additional security approval to deploy templated applications and hosts through the use of standard, reusable patterns.
3. Improve security posture by requiring managed firewalls on hosts.
4. Increase specificity of access filters as network traffic passes through multiple layers of filtering (i.e. most specific filtering takes place closest to the application and data being protected), minimizing the need to make changes that have the potential to impact many hosts/services.
5. Expand data center fingerprint scanning to all data center zones included in this document. https://drive.google.com/open?id=0B1XDrjM7mIeSb2NndjJ0NmtPNG8&authuser=0



Definitions

Standard (Big/Non-Enterprise) Zone (SZ)

1. Hosts for applications that contain **internal** or **public** data (no **sensitive** or **confidential** data) should be placed in the Standard Zone, including database hosts.
2. The Standard Zone will have a blacklist of specific ports that are blocked inbound from non-datacenter networks.
    a. The list of blocked ports will consist of a list of ports based on data from PaIRS and represents the top ports being scanned at the University. Additional ports may be added/removed as conditions change. See Appendix E for the initial port list and additional information.
    b. If applications require permitting one of the above ports, the requirement must be documented in the application requirements document during application design.
    c. Requests to permit traffic for one of these ports must be submitted to the NOC. No security approval is necessary.

CI Enterprise Zone (EZ)

1. Applications that handle **sensitive** or **confidential** data should be placed in the EZ. The database host for these servers should be placed in the HEZ (see below).
2. Standard Enterprise Zone permits all traffic from other datacenter networks. The HEZ only permits traffic from the Enterprise Zone
3. CI servers must use puppet for IPTables or Windows Firewall configuration if they are placed in the CI Enterprise Zone.
4. Router ACLs permit all traffic between datacenter networks and LTM networks.
    a. Current list of datacenter networks documented in Appendix A.
    b. Includes infrastructure traffic (monitoring, authentication, etc)
5. Host-specific network ACL rules are required for any access from outside the datacenter to the EZ network.
6. Equivalent to Legacy EZ for security monitoring purposes
7. Rationale
    a. Provides an additional layer of security between hosts in the non-EZ and the HEZ.
    b. Permits visibility into traffic between non-EZ and HEZ hosts
    c. Allows for installation of a firewall in the future without renumbering hosts.
    d. Provides a scalable and maintainable security posture.

High-security Enterprise Zone (HEZ)

1. Database hosts that store **sensitive** or **confidential** data should be placed in the HEZ.
2. Hosts that require Internet access **should not** be placed in the HEZ.
    a. Permits for Internet IPs to communicate with HEZ hosts must be as specific as possible and the Internet host must be a server, not a user workstation.
    b. HEZ Internet permits will only be granted in very specific circumstances and must be approved by security and receive a dispensation from the Enterprise Architecture Steering Committee.
3. HEZ hosts should use 10-net IP space where possible
4. No connections between hosts in the HEZ and the LTM are permitted.
5. Default permit for traffic from the EZ to the HEZ
6. Other access for the HEZ network are default deny; all traffic must be explicitly permitted.
7. Infrastructure traffic (monitoring, authentication, etc) will be permitted for all hosts, and implemented for the entire subnet.

Infrastructure and Admin traffic

1. Traffic that is common to many hosts in a zone should be configured for all hosts in that zone. IPtables on individual hosts will prohibit traffic not explicitly required.
   e.g., UC4 should be permitted to talk to anything on UC4 ports (2217, 2218), though UC4 may not be used on all hosts.
2. Permits for developer and administrator workstations are prohibited. Administrators should use bastion hosts to run management applications.

215 Network Zone

1. CI hosts that meet EZ criteria and do not have iptables configuration enforced via a centralized configuration management tool must be placed in the 215 network.
2. All application- or host-specific router traffic must be explicitly permitted in the router ACL.
3. New hosts should conform to new security guidelines, including configuration management, and should be placed in the CI EZ or HEZ. The 215 network should only be used as a last resort.
4. Hosts currently in the 215 network (ARC and PAC hosts) should migrate to the CI EZ when possible.

Proposed ACL Management Policy for CI Migrations

1. Migration teams will document network traffic requirements during the discovery phase.
2. Migration teams will deliver network traffic documentation to the systems team and the network team for review.
3. Systems team will create puppet configuration templates for the applications.
4. Network team will create ACL rules using object groups
    a. Create a IOS object group for each application and tier (eg ‘ARC-WEB’)
    b. Future environments should be deployed by only updating the object groups

Deployment

1. Implement new CI EZ to segregate non-puppet CI hosts from puppet CI hosts
    a. Propose 128.59.94.0/24, with 128.59.95.0/24 reserved for expansion.
2. Supplement existing security design to include a High Security Enterprise Zone in addition to the EZ
    a. Propose 10-net IP network

   b. Propose 128.59.212.0/24 Use updated ACL policies, in conjunction with puppet IPTables management and enforcement, to ensure appropriate host security.
   c. See proposed policy below

Issues (Draft)

1. Software updates for hosts using net10 IPs (in the HEZ)
2. Puppet generation of IP tables configs
3. Management access to servers/infrastructure. Options include:
   a. VPN specific to infrastructure
   b. Bastion/jump host(s)
4. Existing exceptions to rules for non-CUIT staff (e.g. ARC spreadsheet upload tool)
5. Standard process and design for security exceptions
6. Different security design for dev/test environments?
7. Need to consider security for storage devices (all CI data is stored on CI NetApps) and differentiate file services (e.g. CIFS) from VMDK, DB infrastructure.
8. Need to consider security for alternate host access (e.g. console access)

References

1. http://policylibrary.columbia.edu/data-classification-policy
2. http://policylibrary.columbia.edu/registration-and-protection-systems-policy
3. Network Security Recommendations

Appendix A

Datacenter networks, as of 2015-01
128.59.1.0/24 -- Morningside Network Infrastructure (DNS & DHCP)
128.59.40.0/24 -- Legacy “DMZ”
128.59.48.0/24 -- CSM VServers
128.59.59.0/24 -- Legacy “DMZ”
128.59.62.0/24 -- Legacy “DMZ”
128.59.92.0/24 -- CI “DMZ”
128.59.213.0/24 -- Legacy Enterprise Zone
128.59.214.0/24 -- Legacy Enterprise Zone
128.59.215.0/24 -- CI Enterprise Zone -- deprecated
128.59.105.0/24 -- LTM VServers

Proposed new subnets
128.59.212.0/24 -- HEZ
128.59.94.0/24 -- CI EZ

Appendix B - Data Classification Mapping

Data Classifications can be found in the CU Policy Library:
http://policylibrary.columbia.edu/data-classification-policy

Data Classification	Server Type	Zone
Sensitive OR Confidential	Web	EZ
	Application	EZ
	Database	HEZ
Internal OR Public	Web	SZ
	Application	SZ
	Database	SZ

Appendix C -- ACL Implementation Detail

ACL's are implemented on the data center distribution routers. ACL's are applied in the VLAN interface outbound direction only, ie, traffic is filtered from the router to the servers.

Appendix D -- Access matrix

SOURCE → ↓ DEST	Internet	Campus	DC non-EZ	EZ	HEZ
Internet	N/A	N/A	open	requires permit	NO
Campus	N/A	N/A	open	requires permit	requires permit
DC non-EZ	port blacklist	port blacklist	open	open	requires permit
EZ	requires permit	requires permit	open	open	open
HEZ	NO	requires permit	requires permit	open	open

Appendix E -- Port blacklist

Port blacklist as of v.0.31 of document:
21 -- FTP default port
23 -- Telnet default port
139 -- NetBIOS session service
445 -- SMB file sharing service default port
1433 -- MSSQL default port
3306 -- MYSQL default port
3389 -- RDP default port
5060 -- SIP default port
5900 -- VNC default port
9200 -- Elastic Search default port

ajohnson, m bhalodkar, j rosenblatt, jrini, c eigen, s singh, a crosswell

Document Control

Editor	Version	Date	Approved	
aj316	0.1	2015-01-26		Initial version
aj316	0.2	2015-03-20		Updated with changes for additional security in Standard Zone
aj316	0.3	2015-04-28		Numerous changes, Medha, Joel, Alan, Joe R, Tony J
aj316	0.4	2015-05-27		Accepted comments from Alan C, Joel R, Dave C, Zahid M.
aj316	0.41	2015-05-27		Moved port blacklist to Appendix
aj316	0.42	2015-05-28		Minor edits: cleaned up footnotes
aj316	1.0	2015-05-28		Reviewed with execs
aj316	1.1	2015-06-04		Fix description for port TCP/1433