Decision tree and job aid for
LAN Administrators

InterZone Migrations: Deadline is October 2023
InterZone decision tree:
In Presentation mode, hover around each element on the decision tree and 🖤 to obtain more information.
Type of device
Systems vs. User devices

Type of device

A primary goal of the network separation is to separate user systems from server systems. Identify if your device(s) are a System device or a User Interactive device.

• **User Interactive device**
  • A user system where a user tends to interact with the system with a local human interface device (keyboard, mouse, etc.). Usually leveraged for general computing.

• **System device**
  • A system device which tends to have a specific purpose and/or provide services remotely over the network. Typically servers, purpose-specific devices (including IoT), etc.
User systems:
A question of management

User systems come under different levels of trust, primarily when it comes to levels of management.

**Decision already taken**
- User Interactive device = YES

**Current decision**
- Determine if it is a McGill Managed device
  - No: Determine if the user is still a McGill user
  - Yes: Determine the level of structure required to manage the user
Managed User Systems
Structured or Not?

Decision Already Taken
• User Interactive Device = YES
• McGill Managed = YES

Current Decision
• Does the user system require more structure?
  • Yes: Registered
  • No: User Secure

Characteristics of a device requiring structure:
• Requires regular admin organization where systems have specific needs to be grouped or managed more closely.
  • Acting as a server to provide service(s) over the network. Can allow for inbound access with control and registration
  • Compliance requirements for more Granular Protection
  • Isolation requirements as systems are not able to be maintained securely (patches, etc.) and require additional protection
• Similar to current VLAN management
• Does not gain user mobility/unified experience over different connection types
Zone: User Secure
Managed Users

Decision to get here
• User Interactive device = YES
• McGill Managed = YES
• Requires structure = NO

Zone: User Secure
• Users on managed devices
  Examples: Administrative staff, faculty, supported researchers
• Users and systems have a registered technical admin (ITS, Faculty Admin, LAN Admin, Lab Admin, etc.) and are maintained
• Dynamic allocation (DHCP/non static, mobile)
• Primarily accessing services: Outbound Internet access, no direct incoming connections
Zone: Registered
Additional information on decision tree path

Decision to get here
• User Interactive device = YES
• McGill Managed = YES
• Does the device require structure? YES
• Zone: Registered

Examples: Student/research labs, departmental servers, special devices
• Supported systems with registered admins and required structure;
  • provide services over the network,
  • requires more static structure (static IP addressing)
  • more controlled isolation.
• Can allow for inbound access with control and registration
• Similar to current VLAN management.
• Required to comply with upcoming policies/technical controls
Unmanaged user systems: McGill Users or Not?

While a user system may not be managed, we still need to identify if this is a McGill user or not as McGill users receive a different level of privileges and permissions.

**Decision already taken**
- User Interactive device = YES
- McGill Managed = No

**Current decision**
- Is this still a McGill User?
  - No: Guest Zone
  - Yes: Decision Point > Unmanaged Affiliate
Unmanaged User System
Affiliate or general User

Where does the system go?

Decision tree path:
  • User Interactive Device = YES
  • McGill Managed = NO
  • McGill User = YES
  • Determine if it is an Unmanaged Affiliate or not.

  • Follow the path once you have determined if YES or NO.
Zone: Guest
Non-McGill users, self registration, Eduroam

Where does the system go?

Decision tree path:
• User Interactive Device = YES
• McGill Managed = NO
• McGill User = NO
After following the path, if it is determined that it is not a McGill user, do the following:
Assign to GUEST Network Zone

GUEST
• Characteristics
  • Guest users have no current affiliation to McGill
  • They have limited access to McGill resources
  • No access to McGill resources other than DMZ (public)
  • No McGill AD access
  • Not classified within the McGill IP space
  • Access is limited to reduce the possibility of compromising McGill resources while accessing public resources.
  • Users on an isolated network with only Internet access.

Examples: Eduroam, guest WiFi for conferences

BACK TO INTERZONE DECISION TREE
Decision: McGill User or Affiliate
Determine if they are not covered by the legal definition of McGill

Where does the system go?
Decision tree path:
- User Interactive Device = YES
- McGill Managed = NO
- McGill User = YES
- Unmanaged Affiliate? = YES or NO

- Follow the path once you determine if it is an Unmanaged Affiliate or not
Zone: User (Group: General)

General unmanaged McGill users

Where does the system go?

Decision tree path:

- User Interactive Device = YES
- McGill Managed = NO
- McGill User = YES
- Unmanaged Affiliate? = NO

After following the path, if it is determined that it is a not a managed Affiliate

Then assign to User Network Zone

Characteristics:

Unmanaged users on non-compliant devices who have little support

Examples: Students, unmanaged staff, course lecturers, student organizations/clubs (Internet access only)

- Bring Your Own Devices (BYOD)/unmanaged systems

Additional information

- Permissions include the following:
  - Includes Office365, Desire2Learn (D2L), and sharing to cloud services
  - Public McGill systems, limited access to internal Applications
  - No direct Active Directory (AD) access but still treated as McGill access
Zone: User (Group: Affiliate)
Unmanaged Affiliate Users

Where does the system go?

Decision Tree path:

- User Interactive Device = YES
- McGill Managed = NO
- McGill User = YES
- Unmanaged Affiliate? = YES

After following the path and it is determined that it is a managed Affiliate then:

Then assign to User Network Zone

BACK TO INTERZONE DECISION TREE
InterZone decision tree:
Additional information on decision tree path

Where does the system go?

Decision Tree path;
• User Interactive Device = NO
• Determine if it is a McGill Managed device
• Follow the path for YES or NO
Zone: Partner
Additional information on decision tree path

Where does the system go?

Decision tree path:
• User Interactive Device = NO
• McGill Managed = NO

After following the path and it is determined that it not McGill Managed:
Assign to PARTNER Network Zone

• Characteristics
  • Registered devices loosely affiliated with McGill but managed and supported externally
  • Requires registered contacts (internal & external)
  • No AD integration (preferred)
  • Not classified within the McGill core Public IP Space

Examples: McGill Partners, Food Services contracts, 3rd party public displays
Zone: Infra (Decision)
Additional information on decision tree path

Where does the system go?
Decision tree path:
• User Interactive Device = NO
• McGill Managed = YES
• Is it a Core Network?

After following the path and it is determined that it is a Core Network:

Assign to INFRA Network Zone

INFRA
• Examples :
  • Network Infrastructure devices (firewalls/routers/switches)
InterZone decision tree:
Additional information on decision tree path

Where does the system go?

Decision tree path:
• User Interactive Device = NO
• McGill Managed = YES
• PCI? = YES

After following the path and it is determined that it is PCI:

Assign to PCI Network Zone

PCI
• Examples:
  • Network for systems within PCI scope (ex: Moneris PinPads)
InterZone decision tree:
Additional information on decision tree path

Where does the system go?
Decision tree path:
• User Interactive Device = NO
• McGill Managed = YES
• Physical Safety? = YES

After following the path and it is determined that it is Physical Safety:
Assign to SAFETY Network Zone

SAFETY
• Examples:
  • Campus Safety (including card readers and surveillance)
InterZone decision tree: 
Additional information on decision tree path

Where does the system go?

Decision Tree path:
• User Interactive Device = NO, System Device = YES
• McGill Managed = YES

After following the path and it is determined that it is
• Central IoT Service? = YES

After following the path and it is determined that it is a Central IoT Service:
Assign to DEVICE Network Zone

Characteristics
• Devices distributed all over campus
• Standardized access requirements
• Centralized management
• Device profiling

Examples: ITS and some FMAS managed devices only (i.e. Wireless Access Points, Crestron, uPrint, etc), facility devices managed by ITS (i.e. HVAC)
InterZone decision tree:
Additional information on decision tree path

Where does the system go?

Decision tree path:
- User Interactive Device = NO
- McGill Managed = YES
- Central IoT Service?

After following the path to determine whether it is a Central IoT service or not:

Follow the path for YES or NO
InterZone decision tree:
Additional information on decision tree path

Where does the system go?

Decision Tree path:
• User Interactive Device = NO
• McGill Managed = YES
• Central IoT Service? = NO

After following the path and it is determined that it is not a Central IoT service:
Assign to REGISTERED Network Zone