Objective for today

- For the Network Upgrade & Information Security project to
  - Share project information and updates
  - Create more awareness on upcoming changes & functionality in scope
    - special focus 3-tiers of Next Generation Firewalls

Information sharing…
- Allow the project team to
  - Identify areas of collaboration & support
  - Gain your important feedback
Logistics & Information

- We have the time we need!
  - Presentation of 1 hour & then 30 mins for questions...
  - Room is available after 90 mins

- Please ask your questions anytime throughout the presentation

- Please fill in the attendance sheet

- The presentation will be available on our project website

- Bathroom location & keys
<table>
<thead>
<tr>
<th>Subject</th>
<th>Duration</th>
<th>Presenter(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction</td>
<td>10 minutes</td>
<td>Josee and all</td>
</tr>
<tr>
<td>2. Project Scope Re-cap &amp; Timeline</td>
<td>5 minutes</td>
<td>Josee Daoust</td>
</tr>
<tr>
<td>3. Wired &amp; Wireless Deployment</td>
<td>5 minutes</td>
<td>Josee Daoust</td>
</tr>
<tr>
<td>4. Updates:</td>
<td>10 minutes</td>
<td>Spiro Mitsialis</td>
</tr>
<tr>
<td>I. Network Change &amp; Configuration Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. DDI Solution (DHCP, DNS, IP Change Management)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Wireless Improvements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Next Generation Firewalls:</td>
<td>35 minutes</td>
<td>Spiro Mitsialis, Hayson Wong</td>
</tr>
<tr>
<td>I. Internet Edge</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. MPLS Network &amp; Inter Zone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Datacenter design</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Alignment to other ITS initiatives:</td>
<td>10 minutes</td>
<td>Hayson Wong</td>
</tr>
<tr>
<td>I. Identify and Access Management (IAM) &amp; Multi Factor Authentication (MFA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. Information Technology Service Management (ITSM)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Unified Communications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Question and Answer Period</td>
<td>15 minutes</td>
<td>All</td>
</tr>
<tr>
<td>8. Closure:</td>
<td>5 minutes</td>
<td>Uma Viswanathan, Josee Daoust</td>
</tr>
<tr>
<td>I. Key points to remember</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. Post Presentation Survey</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Word of Thanks</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Introduction

• Introduction of Today’s Presenters

• Quick Round Table
  • Your Name
  • Your Role
  • Your Department/Faculty
2. Project Scope Recap & Timeline:
Network Upgrade Project & Information Security Project

<table>
<thead>
<tr>
<th>Subject</th>
<th>Duration</th>
<th>Presenter(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction</td>
<td>10 minutes</td>
<td>Josee and all</td>
</tr>
<tr>
<td>2. <strong>Project Scope Recap &amp; Timeline</strong></td>
<td>5 minutes</td>
<td>Josee Daoust</td>
</tr>
<tr>
<td>3. Wired &amp; Wireless Deployment</td>
<td>5 minutes</td>
<td>Josee Daoust</td>
</tr>
<tr>
<td>4. Updates:</td>
<td>10 minutes</td>
<td>Spiro Mitsialis</td>
</tr>
<tr>
<td>I. Network Change &amp; Configuration Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. DDI Solution (DHCP, DNS, IP Change Management)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Wireless Improvements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Next Generation Firewalls:</td>
<td>35 minutes</td>
<td>Spiro Mitsialis, Hayson Wong</td>
</tr>
<tr>
<td>I. Internet Edge</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. MPLS Network &amp; Inter Zone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Datacenter design</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Alignment to other ITS initiatives:</td>
<td>10 minutes</td>
<td>Hayson Wong</td>
</tr>
<tr>
<td>I. Identify and Access Management (IAM) &amp; Multi Factor Authentication (MFA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. Information Technology Service Management (ITSM)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Unified Communications (UC)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Question and Answer Period</td>
<td>15 minutes</td>
<td>All</td>
</tr>
<tr>
<td>8. Closure:</td>
<td>5 minutes</td>
<td>Uma Viswanathan, Josee Daoust</td>
</tr>
<tr>
<td>I. Key points to remember</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. Post Presentation Survey</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Word of Thanks</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Project Scope Re-cap: Network Upgrade Overview

LEGEND:
- ** CFT: Call for Tender
- ** NCCM: Network Change & Config Management

Network Upgrade Project

- Wired Network Upgrade
  - Dist& CORE Layer
  - Access Layer
  - Inter Zone Routing
  - Data Center

- Physical Infrastructure
  - Telecom Room Construct
  - Fiber Cabling
  - Fiber

- Wireless
  - Replace/ Add Access Points
  - Upgrade Controllers
  - Outdoor WIFI

- Management & Monitoring
  - Work Order System
  - NCCM (Webtools replacement)

- System Work Order
  - Edge Routing
  - DDI Solution
  - IPAM
  - DHCP
  - DNS

- Access
  - DDI Solution
  - Fiber

- Cabling
  - Cabling

- Physical Infrastructure
  - Telecom Room Construct
  - Fiber
  - *CFT C0000250
  - *CFT C0000497

- *CFT C0000127
  - Upgrade Controllers
  - Outdoor WIFI

- NCCM (Webtools replacement)
  - NCCM

- Ongoing
  - CFT

- Completed
  - CFT

- *CFT

- ** NCCM

- Call for Tender

- Network Change & Config Management
Project Scope Re-cap:
Information Security Overview

Main Focus today:

- Internet Edge
- Inter-Zone
- Data Center
- Campus Migrations
- Enterprise Server Migration
- Next Gen Firewalls & Intrusion Prevention System
- Cisco Stealthwatch
- Security Info & Event Management (SIEM)
- Anti-virus & Malware Protection
- Network Access Control (NAC)
- 802.1x
- Compliance
- HW Solution
- Integration

LEGEND:
- ONGOING
- COMPLETED

REMINDER:
Decommissioning of Trend Micro Antivirus solutions from McGill-managed computers (Oct/18) & Trend Home Edition (Dec/18)

*CFT: Call for Tender
**SCEP: System Center End Point Protection
Resource availability remains a high risk to maintain the overall schedule. Team members share workload between Operational and Project tasks.
### 3. Wired and Wireless Deployment

<table>
<thead>
<tr>
<th>Subject</th>
<th>Duration</th>
<th>Presenter(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction</td>
<td>10 minutes</td>
<td>Josee and all</td>
</tr>
<tr>
<td>2. Project Scope Re-cap &amp; Timeline</td>
<td>5 minutes</td>
<td>Josee Daoust</td>
</tr>
<tr>
<td><strong>3. Wired &amp; Wireless Deployment</strong></td>
<td>5 minutes</td>
<td>Josee Daoust</td>
</tr>
<tr>
<td>4. Updates:</td>
<td></td>
<td>Spiro Mitsialis</td>
</tr>
<tr>
<td>I. Network Change &amp; Configuration Management</td>
<td>10 minutes</td>
<td>Spiro Mitsialis</td>
</tr>
<tr>
<td>II. DDI Solution (DHCP, DNS, IP Change Management)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Wireless Improvements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Next Generation Firewalls:</td>
<td>35 minutes</td>
<td>Spiro Mitsialis, Hayson Wong</td>
</tr>
<tr>
<td>I. Internet Edge</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. MPLS Network &amp; Inter Zone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Datacenter design</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Alignment to other ITS initiatives:</td>
<td>10 minutes</td>
<td>Hayson Wong</td>
</tr>
<tr>
<td>I. Identify and Access Management (IAM) &amp; Multi Factor Authentication (MFA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. Information Technology Service Management (ITSM)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Unified Communications (UC)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Question and Answer Period</td>
<td>15 minutes</td>
<td>All</td>
</tr>
<tr>
<td>8. Closure:</td>
<td>5 minutes</td>
<td>Uma Viswanathan, Josee Daoust</td>
</tr>
<tr>
<td>I. Key points to remember</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. Post Presentation Survey</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Word of Thanks</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Wired and Wireless Deployment – Status
Downtown campus

Residence Buildings:
• Completed Sept 2017

North-West District Buildings:
• Will finish Mid-Dec 2018, except:
  • Education: Floors 1 & below
  • Stewart Biology

North-East Priority Buildings:
• Montreal Genomics and Proteonics Center
• Currie Gymnasium

Off-Campus Buildings:
• Being done in parallel to other districts
Wired and Wireless Deployment – Status
Macdonald campus

Residence Buildings:
• Started June 2017
• Completed May 2018 (as Ecorez 1 & 2 was deferred)

Deployment plans:
• Start in 2020
• address urgencies before if they arise
### 4. Updates – 1. Network Change & Configuration Management (NCCM)  
2. DDI Solution and 3. Wireless Improvements

<table>
<thead>
<tr>
<th>Subject</th>
<th>Duration</th>
<th>Presenter(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Introduction</strong></td>
<td>10 minutes</td>
<td>Josee and all</td>
</tr>
<tr>
<td><strong>2. Project Scope Re-cap &amp; Timeline</strong></td>
<td>5 minutes</td>
<td>Josee Daoust</td>
</tr>
<tr>
<td><strong>3. Wired &amp; Wireless Deployment</strong></td>
<td>5 minutes</td>
<td>Josee Daoust</td>
</tr>
<tr>
<td><strong>4. Updates:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I. Network Change &amp; Configuration Management</td>
<td>10 minutes</td>
<td>Spiro Mitsialis</td>
</tr>
<tr>
<td>II. DDI Solution (DHCP, DNS, IP Change Management)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Wireless Improvements</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>5. Next Generation Firewalls:</strong></td>
<td>35 minutes</td>
<td>Spiro Mitsialis, Hayson Wong</td>
</tr>
<tr>
<td>I. Internet Edge</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. MPLS Network &amp; Inter Zone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Datacenter design</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>6. Alignment to other ITS initiatives:</strong></td>
<td>10 minutes</td>
<td>Hayson Wong</td>
</tr>
<tr>
<td>I. Identify and Access Management (IAM) &amp; Multi Factor Authentication (MFA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. Information Technology Service Management (ITSM)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Unified Communications (UC)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>7. Question and Answer Period</strong></td>
<td>15 minutes</td>
<td>All</td>
</tr>
<tr>
<td><strong>8. Closure:</strong></td>
<td>5 minutes</td>
<td>Uma Viswanathan, Josee Daoust</td>
</tr>
<tr>
<td>I. Key points to remember</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. Post Presentation Survey</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Word of Thanks</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Network Change & Configuration Management (NCCM)

- WebTools Replacement
- Modern User Interface
- Ansible backend
- Integration
  - DDI, ICINGA, Libre NMS, Logs
- New Features
  - Automation/Workflows
  - Configure Multiple Ports
  - L2 Security, dot1x and more
- More troubleshooting
  - Switch port Info
  - RRD Graphs
  - Logs
  - User Identification (dot1x)
DDI (DHCP, DNS, IP Address Management)

• Many units have moved to DDI
• Bugs (we have escalated the cases)
  • DHCP to IPAM
  • NetChange to IPAM

Internal – External DNS Example
• Internal: adfs.mcgill.ca 132.216.75.190
  • More trusted access: fewer security controls
• External: adfs.mcgill.ca 132.206.11.25
  • Less trusted access: Extra layer of security (e.g. soft lock for Office365)

• Cleanup of External DNS
  • Generally internal device should NOT be accessible from Internet

• Major upgrade to version 7.x in 1H 2019
• Your Feedback (upcoming survey)
Guest Network

- **Guest – Improve Security**
  - Access to McGill resources as if external
  - Includes Eduroam users
  - Simplify Access

- **New Portal (Aruba Clearpass)**
  - Self Registration
  - Social Media Login
    - Facebook, Google, Instagram, Twitter, Microsoft, LinkedIn

- **To replace** https://search.mcgill.ca
  - Replace “Wireless Access Only” access for now
  - Evaluate Sponsored Guest

Wireless and McGill Network *(provides access to resources on the McGill network, departmental shares, etc.)*
Wireless

- 300 Series **Access Points** (APs) (802.11ac wave 2)
  - Potential for real world 600 Mbps vs ~ 200 Mbps on 802.11n
  - Beamforming – Throughput does NOT degrade as client moves farther from AP
  - Multi-User MIMO – AP acts like switch; transmit 4 simultaneous streams
    - Receive still single stream
    - Not many clients support wave 2 yet

- AOS 8.x
  - Clustering of controllers
  - Zero downtime Firmware upgrades (we hope)
    - Half of AP’s upgraded at one time; always an AP to take up the slack
    - Coverage dependent
  - Easier Management
  - Only for new 300 series AP’s

- Outdoor Coverage
  - Outside Leacock by picnic tables (delayed due construction)
  - James Square
  - Otto Maas/Burnside Hall terrace
  - More to come next year
### 5. Next Generation Firewalls:
Internet Edge, MPLS & Inter Zone and Datacenter

<table>
<thead>
<tr>
<th>Subject</th>
<th>Duration</th>
<th>Presenter(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction</td>
<td>10 minutes</td>
<td>Josee and all</td>
</tr>
<tr>
<td>2. Project Scope Re-cap &amp; Timeline</td>
<td>5 minutes</td>
<td>Josee Daoust</td>
</tr>
<tr>
<td>3. Wired &amp; Wireless Deployment</td>
<td>5 minutes</td>
<td>Josee Daoust</td>
</tr>
<tr>
<td>4. Updates:</td>
<td>10 minutes</td>
<td>Spiro Mitsialis</td>
</tr>
<tr>
<td>I. Network Change &amp; Configuration Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. DDI Solution (DHCP, DNS, IP Change</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Wireless Improvements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Next Generation Firewalls:</td>
<td>35 minutes</td>
<td>Spiro Mitsialis, Hayson Wong</td>
</tr>
<tr>
<td>I. Internet Edge</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. MPLS Network &amp; Inter Zone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Datacenter design</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Alignment to other ITS initiatives:</td>
<td>10 minutes</td>
<td>Hayson Wong</td>
</tr>
<tr>
<td>I. Identify and Access Management (IAM)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&amp; Multi Factor Authentication (MFA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. Information Technology Service Management (ITSM)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Unified Communications (UC)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Question and Answer Period</td>
<td>15 minutes</td>
<td>All</td>
</tr>
<tr>
<td>8. Closure:</td>
<td>5 minutes</td>
<td>Uma Viswanathan, Josee Daoust</td>
</tr>
<tr>
<td>I. Key points to remember</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. Post Presentation Survey</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Word of Thanks</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Internet Edge, an Update

• The Good: We have a new internet edge since March 2018!
  • Replaced the old routers and IPS devices
  • We have much better protection:
    • Threat Intelligence
    • Sandboxing
    • Better Intrusion Prevention System (IPS) capabilities
    • URL filtering

• The (not so) Bad:
  • Migrated traffic shaping rules were limiting traffic
  • There have been bugs...

• The Ugly:
  • Some bugs have had some impact (SIP, SSL/TLS)
Multi Protocol Label Switching (MPLS) Network

- What is it?
  - Network Virtualization
  - New Inter Zone firewall
- IPv4 & IPv6
- Multicast support
- Today
  - 7 distribution using MPLS
  - Internet Edge zone
  - Inter Zone (F/W)
- Future
  - Dual chassis distribution
  - Farm distribution
  - Access (Wifi) distribution
  - VPN re-design (Q1/2019)
  - Datacenter (2019+)
- Each Zone sees only VLANs within its zone
- Zones talk to other zones via Firewall and FUSION router
- Legacy - default zone for campus
- Students - default zone for Wireless
- Guest - Internet Access only & some Datacenter (DMZ)
The Principles and Constraints

We believe in Security

• Better protect McGill managed systems from unmanaged systems
• Logically Layered Security

Identities are Key

• Communities based on groupings of identities, not individuals
  • Based on logical groupings (apples with apples, oranges with oranges)
  • Move away from “Technical” primary identifiers (ie. Vlan, ip address, etc.)
  • System should only exist in one Zone (VRF) at a time
  • Can be statically assigned, or dynamically (user authentication 802.1X)
  • There will be a logical priority for dynamic access
    • System > Identity
    • Staff > Student > Alumni
The Principles and Constraints Continued.

Design matters, and it’s hard...

• Promote the Client Server model
  • Broadcast domains are dead, long live the internet!
  • Access should work uniformly

• Leverage choke points to improve efficiency
  • Leverage ID Firewalling (AD Groups)
  • Leverage default community rights
  • Global permissions should follow the user
  • More efficient and easier to understand routing and network allocations

• Management is key...
  • Tools and processes will have to be clear to help everyone
Real World Problems... Solved?

• Granting a diverse (Staff, Student) community of users uniform access to ITS or Departmental Servers or Services
  • Consistency
  • Mobility
  • Efficiency
  “I need to move offices for a couple weeks, do I need to request network changes? No? Great!”

• Standardization of Guest Access
  • Eduroam (allows users to gain network access at other institutions)
  • Visitors: social media, etc.
  • Conferences
  “I have to get access for these guests to use the internet, wait, they can do it themselves? Perfect!”
The Zones... At least a start

Free for all:
- Legacy

The Users:
- User
- uSecure
- Guest

The Systems:
- Infra
- Registered
- Partner
- Device
The Datacenter Zones

Crystal ball of the future datacenter, based on the 3-tier model

- Public Facing: DMZ (De-militarized Zone)
- Trusted Apps: Internal Apps
- Protected systems: Sensitive Systems, Backend databases

How should we fit research/academic in?

- Registered (managed)
Legacy

The Legacy (Current McGill) Network(s)

Goal: Transition users and systems into the newly defined zones

• Slowly Recoup IP space for cleaner allocation with migrations
• Eventually reduce and restrict access to sensitive resources and treat as insecure zone -> decommission

• No IPv6
• No identity based rules
User Zone: uSecure

Secure Users that are managed and are compliant to McGill standards

Goal: to protect properly managed users from the unmanaged systems while providing unified experience and mobility

Examples: Administrative Staff, Faculty, Supported Researchers

• Dynamic allocation (DHCP/non static, mobile)
• Users must have a registered Technical Admin (ITS, Faculty Admin, Lan Admin, Lab Admin, etc.)
• Outbound Internet access, no direct incoming connections
• Will have access to internal applications
• Will be permitted to have AD access
User Zone: User

Unmanaged users who have little support and pose higher risk.

Goal: To provide access to necessary resources, but prevent them from interacting with more secure systems.

Examples: Students, Unmanaged Staff, course lecturers.

- **Bring Your Own Devices (BYOD)/Unmanaged Systems**
- Access consists of mostly Internet traffic
  - Includes Office365 and Desire2Learn and the push to cloud services
- Accessing public McGill systems or limited access to internal Applications
- Student organizations and/or clubs (internet access only)
- No Direct Active Directory (AD) access but still treated as McGill access
User Zone: Guest

Guest users with no current affiliation to McGill

Goal: To limit access of non-McGill users from attacking McGill resources while providing access to public resources

Examples: Eduroam, Alumni, Conference Guest, Hotel, Social Media

• Short term users
• Outbound Internet Access: Restricted/Limited
• Users treated as Externals: do not access McGill Resources other than DMZ (public)
• McGill users/systems do not connect to guest systems
• No access to McGill AD Domain (AD)
• Not classified within the McGill IP space
System Zone: Registered

Systems with Registered admins where they require structure and are well supported.

Goal: Provide granular protection for registered administrators to control access to managed systems particularly where users need to connect via the network.

Examples: Student/Research Labs, Departmental Servers, Special devices

• Require Registered Admins for accountability
  • Will need to be able to document requirements
• Can allow for inbound access with control and registration
• Similar to current VLAN management.
• Will need to comply with upcoming policies/technical controls
System Zone: Partner

Registered Devices loosely tied to McGill where really managed by external support.

**Goal: provide specific access for non-McGill systems while protecting McGill.**

Examples: McGill Partners, Food Services contracts, 3rd party public displays

- Requires registered contacts (internal & external)
- No AD integration (preferred)
- Not classified within the McGill core Public IP Space
Non-User/Workstation/Server type systems usually distributed around campus.

**Goal: Micro-Segmentation used to provide better isolation (ie. prevent lateral movement)**

Examples: ITS Managed devices (i.e. APs, Crestron, uPrint, etc), Facility devices managed by ITS (i.e. HVAC)

- Devices distributed all over campus
- Standardized access requirements across the board
- Centralized management
- Device profiling
Logical Zone: Secure Management

Not really a zone, but a new concept being introduced to support segregation of duties and support Secure Management

Goal: To provide a robust management process to allow for secure administrative access to supported systems and allow admins to use their workstations more freely.

• Separate systems for privileged tasks: Terminal Servers (RDP/SSH), Virtual Desktop Infrastructure (VDI), Remote App
• Differentiate between normal user and “admin” accounts
  • Separation of credential usage
  • Isolated process and technology to protect privileged administration tasks
• Likely a community in a datacenter zone
• Secure Management zones will be given more trust to facilitate easier management
How does this work?

User Zones

User
- Student
- Unmanaged Staff
- Affiliates

uSecure
- Managed Staff
- Managed Researchers

Guest
- Eduroam
- Visitor
- Conference
- Alumni
- Hotel

System Zones

Access from Zones: User, uSecure

Registered
- Faculty Servers
- Faculty Lab
- Research Lab
- Student Lab
- Special Managed Devices

Partner
- Food Services
- Public Displays
- Elections

Devices
- Printers
- Crestron
- HVAC
How does this work?

User Zones

User
- Student
- Unmanaged Staff
- Affiliates

Vendors/External Support

uSecure
- Managed Staff
- Managed Researchers

Guest
- Eduroam
- Visitor
- Conference
- Alumni
- Hotel

System Zones

Access from Populations

Registered
- Faculty Servers
- Faculty Lab
- Research Lab

Student Lab
- Special Managed Devices

Partner
- Food Services
- Public Displays
- Elections

Devices
- Printers
- Crestron
- HVAC
How does this work?

User Zones

- User
  - Student
  - Unmanaged Staff
  - Affiliates

- uSecure
  - Managed Staff
  - Managed Researchers

- Guest
  - Eduroam
  - Visitor
  - Conference
  - Alumni
  - Hotel

System Zones

- Access from AD Groups: “Faculty/Department”

- Registered
  - Faculty Servers
  - Faculty Lab
  - Research Lab
  - Student Lab
  - Special Managed Devices

- Partner
  - Food Services
  - Public Displays
  - Elections

- Devices
  - Printers
  - Crestron
  - HVAC
## 6. Alignment to Other Initiatives

<table>
<thead>
<tr>
<th>Subject</th>
<th>Duration</th>
<th>Presenter(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction</td>
<td>10 minutes</td>
<td>Josee and all</td>
</tr>
<tr>
<td>2. Project Scope Re-cap &amp; Timeline</td>
<td>5 minutes</td>
<td>Josee Daoust</td>
</tr>
<tr>
<td>3. Wired &amp; Wireless Deployment</td>
<td>5 minutes</td>
<td>Josee Daoust</td>
</tr>
<tr>
<td>4. Updates:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I. Network Change &amp; Configuration</td>
<td>10 minutes</td>
<td>Spiro Mitsialis</td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. DDI Solution (DHCP, DNS, IP Change</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Wireless Improvements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Next Generation Firewalls:</td>
<td>2</td>
<td>Spiro Mitsialis, Hayson Wong</td>
</tr>
<tr>
<td>I. Internet Edge</td>
<td>35 minutes</td>
<td></td>
</tr>
<tr>
<td>II. MPLS Network &amp; Inter Zone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Datacenter design</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Alignment to other ITS initiatives:</td>
<td>10 minutes</td>
<td>Hayson Wong</td>
</tr>
<tr>
<td>I. Identify and Access Management (IAM)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&amp; Multi Factor Authentication (MFA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. Information Technology Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management (ITSM)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Unified Communications (UC)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Question and Answer Period</td>
<td>15 minutes</td>
<td>All</td>
</tr>
<tr>
<td>8. Closure:</td>
<td>5 minutes</td>
<td>Uma Viswanathan, Josee Daoust</td>
</tr>
<tr>
<td>I. Key points to remember</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. Post Presentation Survey</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Word of Thanks</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Other Aligned ITS Initiatives

Identity and Access Management (IAM)
• MultiFactor Authentication
• Sailpoint IIQ – Role Mining, Access Provisioning

IT Service Management (ITSM)
• Improved Service Delivery
  • Process streamlining and redefinition
  • Standardization of requests
  • Increased automation

ITS Guidelines and Procedures
• Collaboratively developing a modern systems administration paradigm
• Providing Administrators with more Information and Tools to help
Unified Communication (UC) Project

Benefits

• Enhanced telephony features: unified messaging, audio conferencing, advanced call forwarding rules, number available on multiple devices

• Enhanced collaboration: online meetings, screen sharing, file transfer, instant messaging, video conferencing, presence

• Work from anywhere: phone number available on any internet connected device (laptop, desktop, smartphone, tablet, etc.)

What does it mean to you?

• Requires centrally managed DHCP

• Potentially requires new software to be deployed

• End-user change management
Unified Communication (UC) Project

- CFT issued (C0000747) and currently in evaluation process
- Bidder selection expected by February 2019
- Initial Pilot tentatively Fall 2019
# 7. Question and Answer Period

<table>
<thead>
<tr>
<th>Subject</th>
<th>Duration</th>
<th>Presenter(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction</td>
<td>10 minutes</td>
<td>Josee and all</td>
</tr>
<tr>
<td>2. Project Scope Re-cap &amp; Timeline</td>
<td>5 minutes</td>
<td>Josee Daoust</td>
</tr>
<tr>
<td>3. Wired &amp; Wireless Deployment</td>
<td>5 minutes</td>
<td>Josee Daoust</td>
</tr>
<tr>
<td>4. Updates:</td>
<td>10 minutes</td>
<td>Spiro Mitsialis</td>
</tr>
<tr>
<td>I. Network Change &amp; Configuration Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. DDI Solution (DHCP, DNS, IP Change Management)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Wireless Improvements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Next Generation Firewalls:</td>
<td>35 minutes</td>
<td>Spiro Mitsialis, Hayson Wong</td>
</tr>
<tr>
<td>I. Internet Edge</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. MPLS Network &amp; Inter Zone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Datacenter design</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Alignment to other ITS initiatives:</td>
<td>10 minutes</td>
<td>Hayson Wong</td>
</tr>
<tr>
<td>I. Identify and Access Management (IAM) &amp; Multi Factor Authentication (MFA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. Information Technology Service Management (ITSM)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Unified Communications (UC)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Question and Answer Period</td>
<td>15 minutes</td>
<td>All</td>
</tr>
<tr>
<td>8. Closure:</td>
<td>5 minutes</td>
<td>Uma Viswanathan, Josee Daoust</td>
</tr>
<tr>
<td>I. Key points to remember</td>
<td></td>
<td></td>
</tr>
<tr>
<td>II. Post Presentation Survey</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III. Word of Thanks</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Question Period
## 8. Closure
Survey and word of thanks

<table>
<thead>
<tr>
<th>Subject</th>
<th>Duration</th>
<th>Presenter(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction</td>
<td>10 minutes</td>
<td>Josee and all</td>
</tr>
<tr>
<td>2. Project Scope Re-cap &amp; Timeline</td>
<td>5 minutes</td>
<td>Josee Daoust</td>
</tr>
<tr>
<td>3. Wired &amp; Wireless Deployment</td>
<td>5 minutes</td>
<td>Josee Daoust</td>
</tr>
<tr>
<td>4. Updates:</td>
<td>10 minutes</td>
<td>Spiro Mitsialis</td>
</tr>
<tr>
<td>1. Network Change &amp; Configuration Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. DDI Solution (IP Change Management, DNS, DHCP)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Wireless Improvements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Next Generation Firewalls:</td>
<td>35 minutes</td>
<td>Spiro Mitsialis, Hayson Wong</td>
</tr>
<tr>
<td>1. Internet Edge</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. MPLS Network &amp; Inter Zone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Datacenter design</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Alignment to other ITS initiatives:</td>
<td>10 minutes</td>
<td>Hayson Wong</td>
</tr>
<tr>
<td>1. Identify and Access Management (IAM) &amp; Multi Factor Authentication (MFA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Information Technology Service Management (ITSM)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Unified Communications (UC)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Question and Answer Period</td>
<td>15 minutes</td>
<td>All</td>
</tr>
<tr>
<td>8. Closure:</td>
<td>5 minutes</td>
<td>Uma Viswanathan, Josee Daoust</td>
</tr>
<tr>
<td>1. Key Points to Remember &amp; Collaboration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Post Presentation Survey</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Word of Thanks</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Key Points to Remember

• NCCM (replacement of WebTools)
  • New features
  • Augmented troubleshooting capabilities in NetMan

• DDI (DHCP, DNS, IPAM)
  • Known issues – Being fixed
  • Internal & external DNS
    • Cleanup Underway
    • Use ITS Internal DNS to Prevent Problems

• Guest Network
  • Guest Access via Self-Registration and Social Media Login

• Wireless
  • Higher Bandwidth
  • Better signal propagation
  • Increasing outdoor coverage

• Internet Edge Security
  • Better Security
  • Increased ability to track compromised systems

• MPLS, Inter Zone
  • VRFs = Security Zones => Inter Zone
  • Provides dual chassis distribution
  • Redesign VPN with Inter Zone in mind -> Unified Access
Key Points to Remember

• Inter Zone
  • Layered security
  • Unified access via Identities & Communities
  • 3 Key Zones
    User Zones:
    • **Legacy** - Transition users and systems into the newly defined zones
    • **uSecure** - to protect properly managed users from the unmanaged systems while providing unified experience and mobility
    • **User** - provide access to necessary resources, but prevent them from interacting with more secure systems
    • **Guest** - limit access of non-McGill users from monopolizing McGill resources while providing access to public resources

  Systems Zones:
  • **Registered** - Provide granular protection for registered administrators to control access to managed systems particularly where users need to connect via the network
  • **Partner** - provide specific access for special access for non-McGill systems while protecting McGill
  • **Devices** – Micro-Segmentation used to provide better isolation (ie. prevent lateral movement)

  Logical Zone:
  • **Secure Management** - provide a robust management process to allow for secure administrative access to supported systems and allow admins to use their workstations more freely
Collaboration

We need your feedback, suggestions, and participation!

NCCM (WebTools replacement):
   *Have we thought of everything in terms of new features & improvements?*

DDI (IPAM):
   *Your level of satisfaction and interaction?*

Inter Zone:
   *Would you like to participate in the design and development as an early adopter?*

How?
How to reach us

General inquiries

Project email: network.project@mcgill.ca
Project website: mcgill.ca/network-upgrade

To report issues

Contact the IT Service Desk:

itsupport@mcgill.ca
Online Survey

We need your feedback!

• Link to be emailed to session participants
• All responses are anonymous
thank you
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMP</td>
<td>Anti-Malware Protection</td>
</tr>
<tr>
<td>AP</td>
<td>Wireless Access Point</td>
</tr>
<tr>
<td>CFT</td>
<td>Call For Tender</td>
</tr>
<tr>
<td>DDI</td>
<td>DNS, DHCP, IP Management</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized zone</td>
</tr>
<tr>
<td>IAM</td>
<td>Identity and Access Management</td>
</tr>
<tr>
<td>ITSM</td>
<td>Information Technology Service Management</td>
</tr>
<tr>
<td>MFA</td>
<td>Multi-Factor Authentication</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multi Protocol Label Switching</td>
</tr>
<tr>
<td>NCCM</td>
<td>Network Change and Configuration Management</td>
</tr>
<tr>
<td>NetMan</td>
<td>Network Manager</td>
</tr>
<tr>
<td>NGFW</td>
<td>Next Generation Firewall</td>
</tr>
<tr>
<td>SCEP</td>
<td>System Center End Point Protection</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>UC</td>
<td>Unified Communication</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>VDI</td>
<td>Virtual Desktop Infrastructure</td>
</tr>
</tbody>
</table>