WOU: Layered Network Security

Zone: Wifi   Zone: Residence Halls

4. ISE - Network Authentication

Zone: PCI (credit cards)

Zone: Other network zones

The Internet

1. Umbrella (Open DNS)

2. Border Firewall

VPN: Remote Access

3. FirePOWER (Internal Firewalls and Intrusion Protection: ~17k rules)

5. Data Center/Application Security:

- 2FA: 2-factor authentication (Duo)
- System Logs (AP, LDAP, Portal, Web, Security, ...)
- OS Upgrades (Windows Server 2016, ...)
- App Upgrades (SQL Server, etc...)
- Group-based drive/file security
- SSL Always ON
- AccountLookup (password complexity)
- Internal PentrationTesting
- Network Drive Snapshots
- Sophos + InterceptX
- Email Security Appliances (+Archives)
- Physical Access Control & Survelliance
- Secure (VPN) access to Banner (local only)
- (Future): Custom log analysis system
- Daytime monitoring of systems via 4k monitor
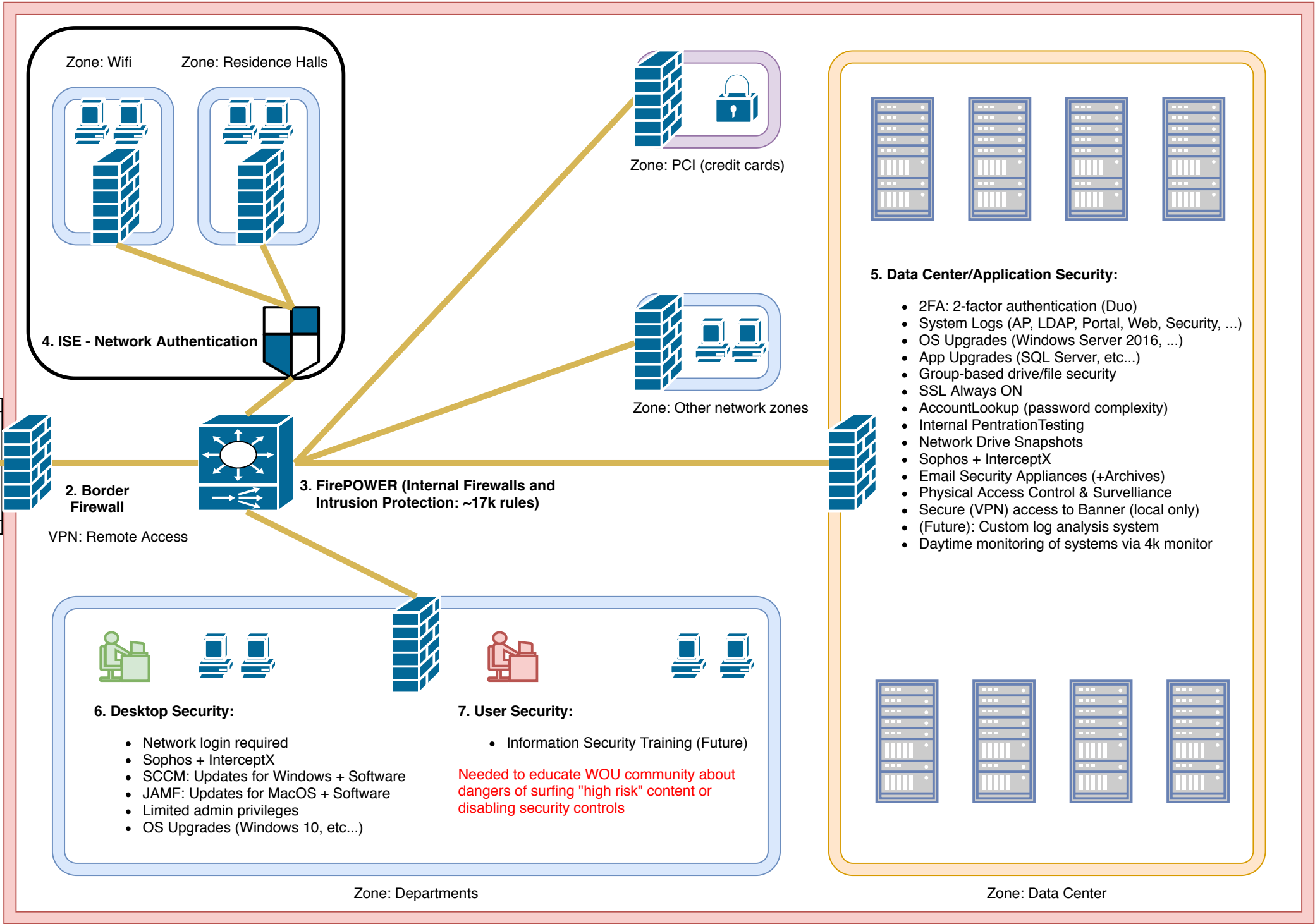
8. External Support:

Penetration Testing (CoalFire)
Vendor Support
Vendor information sessions
Vendor product demonstrations
CIS 20 Framework
PCI education and testing

6. Desktop Security:

- Network login required
- Sophos + InterceptX
- SCCM: Updates for Windows + Software
- JAMF: Updates for MacOS + Software
- Limited admin privileges
- OS Upgrades (Windows 10, etc...)

7. User Security:

- Information Security Training (Future)

Needed to educate WOU community about dangers of surfing "high risk" content or disabling security controls

Zone: Departments

Zone: Data Center