FANSHAWE

INFO-6003

O/S & Application Security

Week 09

Agenda

- Test-02 in Week-11
  - Date Regular Class
  - Time Regular Class
  - Room Regular Room
- General improvements in Windows development since Vista and 2008
- Network Location Awareness and Firewall Profiles
- Network Access Protection

Security Improvements Since Windows Vista/2008 platforms

General Changes

- Many of the security features we see in Windows 7, 8, and 10 / Server 2008 R2 and 2012 R2 were introduced with Vista and Server 2008
- Many changes to default settings
- Security Development Lifecycle plan adopted
- Move towards the principle of least privilege in development of all software
- Software checked against over 1400 threat model scenarios
- All code subject to peer team reviews

Specific Improvements

- Several fundamental changes to the operating system to improve security
  - C++ code enhancements
  - Address space assignments
  - Session Isolation
  - Service hardening
  - Protected processes
  - BitLocker Drive Encryption
  - User Account Control
  - Trusted Installer

C++

- New compiler helps prevent stack based buffer overflows
  - Values are entered into the stack execution space before the return address of the function
  - If the values in the stack are overwritten an error is detected and the program halted
- C library functions such as strcpy that do not adequately validate input have been removed

Memory Randomization

- Address Space Layout Randomization (ASLR)
  - APIs in Kernel32.dll, Winsck32.dll etc. are now loaded at random into one of 256 memory address locations
    - In previous versions of Windows APIs were loaded into well known address locations
    - Malware could locate an API directly by its memory location and bypass security protections
- Memory address pointers and heap memory blocks are obscured
  - Address XORed with random number
  - Feature common in BSD Unix and Linux

ActiveX

- IE can no longer call ActiveX controls
- Many Windows applications have ActiveX controls that were never intended to be called from IE
    - – Microsoft Office applications being called from the browser
- In the past any ActiveX control signed safe for scripting could be executed from another program

BitLocker and TPM

- BitLocker Drive Encryption and TPM
- Available in ultimate & enterprise versions
  - Entire O/S boot volume can be encrypted
  - Cannot boot around the O/S with a Linux boot disk and then access the NTFS files
- File encryption keys are stored on a USB key or on the Motherboard
  - TPM – Trusted Platform Module is a chip on the motherboard that can be used to store encryption keys
  - Encryption keys are retrieved by OS, when it loads, from TPM or USB key, or the user can be prompted for a PIN

Security Improvements in Windows 10

- Identity & Access Control
  - Microsoft introduced new features that take advantage of multifactor authentication (MFA)
  - Credential Guard was also added which uses virtualization-based security (VBS) to protect user's credentials
  - This can also protect local administrator credentials for domain connected computers

Security Improvements in Windows 10

- Identity & Access Control
  - Microsoft Hello can assist with MFA when used on biometric-capable devices
  - Microsoft Passport allows for single sign-on (SSO) and prevents the user from having to retype their password
  - Biometric devices can be used to verify credentials when higher level resources need to be accessed

Security Improvements in Windows 10

- Brute Force Attack Resistance
  - If TPM is used on the machine, the administrator can enable a higher level of account lock-out policy
  - If the O/S detects a brute force attempt, the PC will restart and a 48-character recovery code will need to be used before Windows starts normally
  - These settings can be changed in the Local Group Policy Editor in both Windows 8.1 & Windows 10

Security Improvements in Windows 10

- Information Protection
  - File-level encryption with Enterprise Data Protection can keep data encrypted when it leaves a corporate network
  - This is meant to work in conjunction with BitLocker and is an attempt to keep data secure when in transit as well as at rest
  - Users have more options with file encryption and cold boot attack protection in Windows 10

Security Improvements in Windows 10

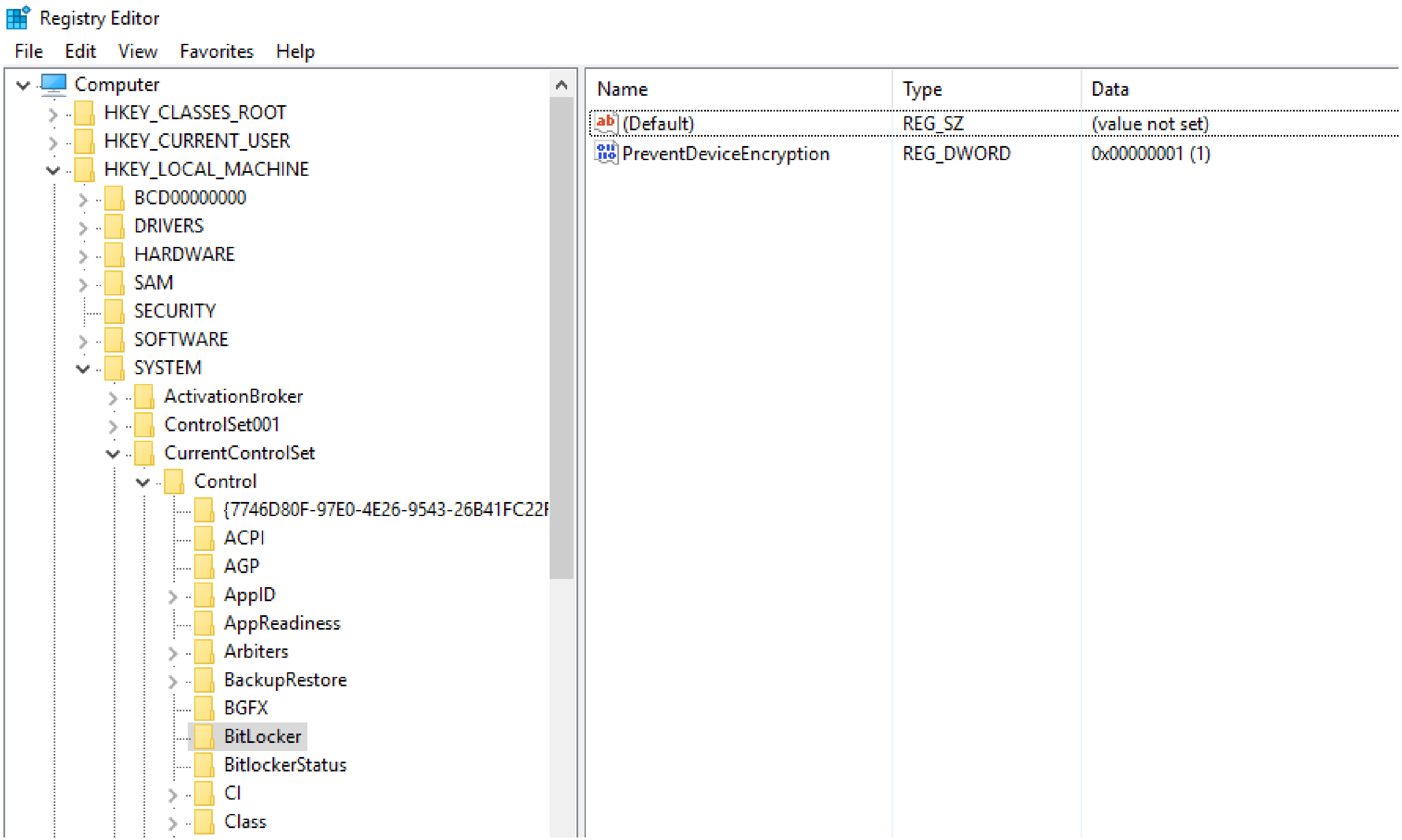
- Information Protection
  - TPM is now handled through the O/S
  - Windows 10 can fully manage BitLocker without the need for changes in BIOS or a system restart
  - Less hassle means more use?

Security Improvements in Windows 10

- Device encryption in the Windows Registry
  - **Subkey**: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BitLocker
  - **Value**:
  - – PreventDeviceEncryption equal to True (1)
  - **Type**:
  - – REG_DWORD

Note: A value of 1 will prevent encryption

BitLocker in Regedit on Windows 10



```
Computer
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
  HKEY_LOCAL_MACHINE
    BCD00000000
    DRIVERS
    HARDWARE
    SAM
    SECURITY
    SOFTWARE
    SYSTEM
      ActivationBroker
      ControlSet001
      CurrentControlSet
        Control
          {7746D80F-97E0-4E26-9543-26B41FC22F
          ACPI
          AGP
          AppID
          AppReadiness
          Arbiters
          BackupRestore
          BGFX
          BitLocker
          BitlockerStatus
          CI
          Class
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
PreventDeviceEncryption	REG_DWORD	0x00000001 (1)

Security Improvements in Windows 10

- Malware Resistance
  - Microsoft revamped its anti-virus protection with a new version of Windows Defender
  - Boot-protection features like Trusted Boot have also received new upgrades
  - Critical system components receive further isolation from other data and potential threats

Security Improvements in Windows 10

- Malware Resistance
  - Microsoft helps prevent Malware starting before the O/S boots up by utilizing features like UEFI Secure Boot
  - Features such as Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP) are used
  - Microsoft Edge replaced Microsoft Internet Explorer with advanced browser extension protection

Security Improvements in Windows 10

- Microsoft Edge
  - Microsoft has made attempts to improve browser security and functionality with this new and improved version of IE
  - Sandboxing is used to try and protect the system from potential vulnerabilities that may exist in browser extensions (Adobe Flash, Java, etc.)

User Account Control

UAC

- User Account Control
- In past version of Windows O/S, users would normally log on as administrators
- Most application assumed the user would have admin privileges to operate
- The user with admin privileges was the largest vulnerability in Windows O/S and applications
- The Run As … command was a previous attempt to allow users to run as a limited user but elevate to administrator for specific tasks

UAC

- User Account Control is an attempt to change user behavior to be more like the Unix/Linux model
  - With Unix and Linux systems most users logon with user credentials and only change to root or SU when admin control is required
- Users can now operate the system with the least privileges required
  - Admin control is not required to surf the net or read e-mail

UAC

- Even the administrators group does not have full administrator token any more
  - By default the Administrators group security token is marked as Deny
    - Referred to as a filtered token
  - Administrators group runs in AdminApproval mode
- If an administrative task needs to be performed, the user needs to elevate the privilege level
  - Secure desktop is used for user rights elevation

UAC

- Each user runs applications in a desktop
- The operating system has its own desktop for security functions
  - Secure desktop hosts the elevated cmd.exe prompt and other system login dialogue boxes
- Once a process is elevated it has the full administrative token
- A limited user that requires elevate privileges will be prompted for an Administrators credentials

UAC Security Issues

- UAC came under some scrutiny as it was fairly easy to turn it off and a lot of users did so because they saw it as a hassle
- Microsoft lowered the intensity of UAC starting with Windows 7
- Most users ignore the warning signs and simply click “ok” and provide the requestor with elevated privileges
- Security Researchers have presented proofs of concept for arbitrary code execution and privilege execution through UAC

Trusted Installer

- Windows Resource Protection
  - Around 70% of the files in the Windows directory are protected
  - Access to change the files is restricted to the TrustedInstaller service
  - Protects Registry Keys
- Prevents Malware from overwriting system files

Coffee Break Reading

- https://en.wikipedia.org/wiki/Cold_boot_attack

Network Location Awareness

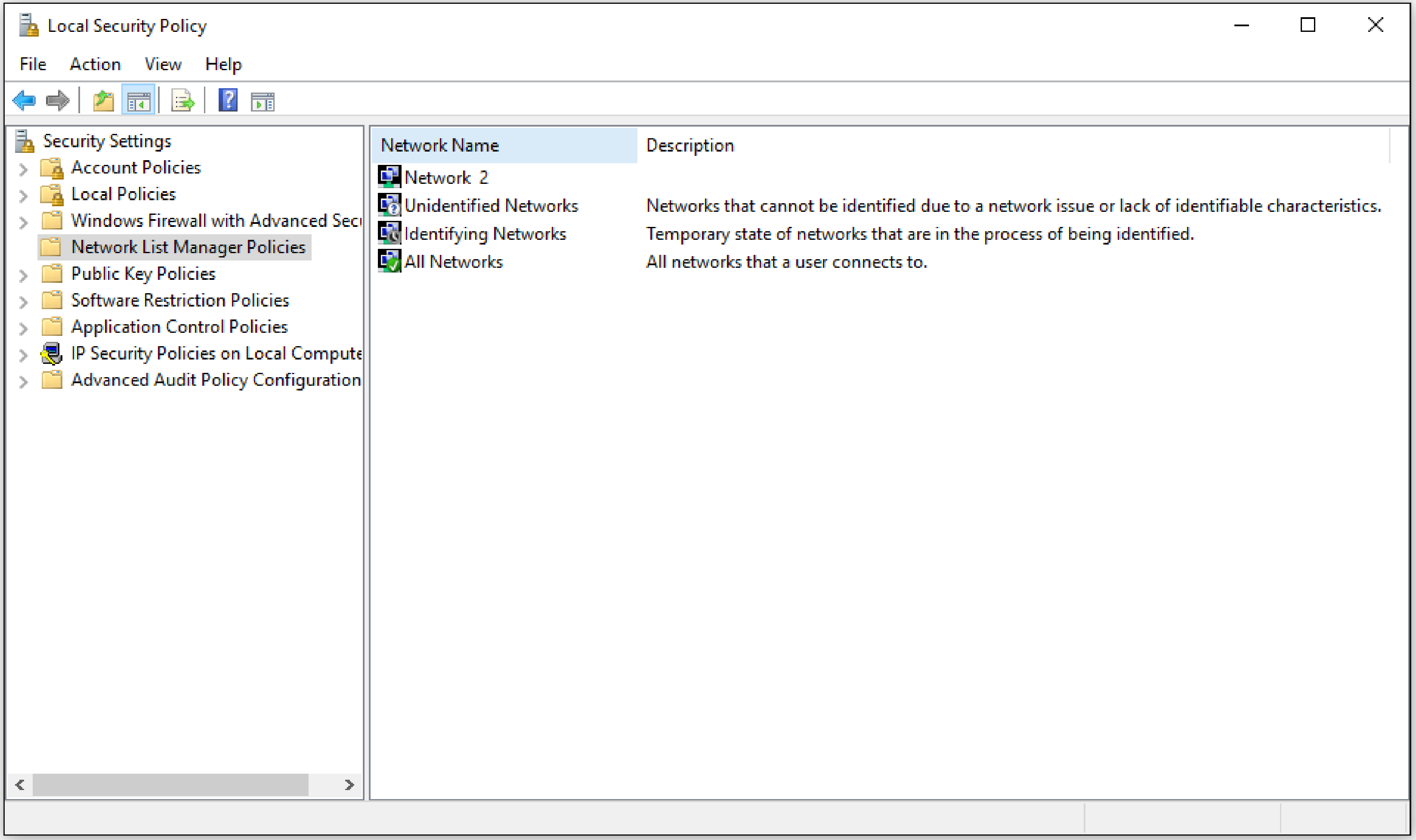
Network Location Awareness

- The goal of NLA is to identify the networks to which a PC is connected
- Based on the network identification the administrator can assign rules for that connection
  - Windows Firewall Profile
- Administrators can tailor the profile to the type of network the PC is connected to:
  - Public: very restrictive
  - Home: less restrictive

Network Location Awareness

- Profiles can be enforced through GPOs
- There are four policies listed in the Security Settings of the Local Security Policy in Windows 10:
  - Network/Domain Name
  - Unidentified Networks
  - Identifying Networks
  - All Networks

NLA Security Settings in Windows 10



Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Firewall with Advanced Seci
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Network Name	Description
Network 2	
Unidentified Networks	Networks that cannot be identified due to a network issue or lack of identifiable characteristics.
Identifying Networks	Temporary state of networks that are in the process of being identified.
All Networks	All networks that a user connects to.

Network Location Awareness

- NLA creates the Network Profile based on the following network characteristics:
  - Managed Network (domain)
  - DC Authenticated
  - Bandwidth of link
  - Primary DNS Suffix (DHCP)
  - Host IP, Subnet IP Address and Mask
  - Default Gateway IP Address
  - MAC Address of DG
  - SSID if Wireless
  - 802.1x Authentication

Network Location Awareness

- Based on Network Characteristics, a globally unique identifier (GUID) is assigned to the Network and stored in Windows
- Sometimes there is not enough information to create a GUID
  - No Default Gateway is one way to get an Unknown or Unidentified Network Type

Network Location Awareness

- If a known network is not detected, or a Domain Controller cannot be contacted, the profile setting that is used will typically be the most restrictive one
- Users have more options now in modern versions of Windows than they had in the days of Windows XP and prior

Windows Firewalls

Firewall Improvements

- Before Windows Vista/2008
  - The firewall is applied to the entire system
  - Only allowed inbound filtering
  - Only had two modes
    - Standard
      - Not on the domain
    - Domain
      - On the domain
      - If the connection specified domain name matched the registry value for the network name the computer assumed it was on the domain

Firewall Improvements

- Windows Vista/2008
  - Multiple Firewall Profiles
    - Domain
      - If the computer is on the domain
      - Managed by the domain admin
    - Public
      - New, or unidentified network
      - Most restrictive profile
    - Private
      - Configured by local admin
      - Tailored to specific network
  - Only one profile can be active at a time

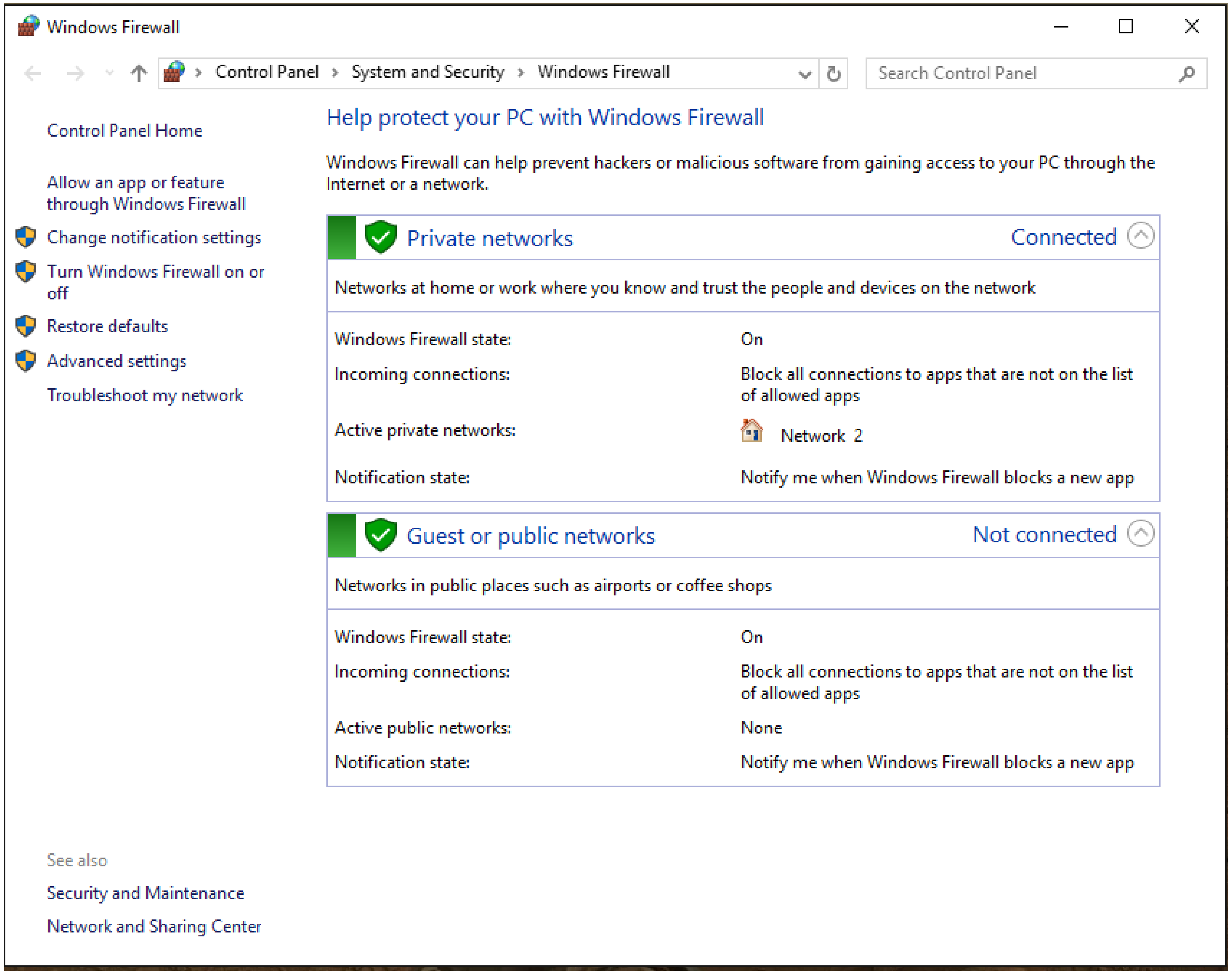
Firewall Improvements

- Since Windows 7/2008R2 the firewall is much more comprehensive
  - Can be attached to multiple networks and each network can have a different firewall profile
    - The three types of network profiles still exist
      - Domain
      - Public
      - Private
    - Private is now subdivided
      - Home: an environment with all trusted computers, usually under your control
      - Work: a work environment, but not on a domain

Multiple Firewall Profiles

- Firewall Profile Determination:
  - Network Location Awareness (NLA) is used to identify the various networks
  - Public by default or Public if no GUID can be determined
  - Domain if the network name defined in the registry matches the one provided through DNS, and the PC can contact the domain controller
  - Private if a GUID can be determined, but the PC is not on a domain
    - Home or Work type chosen by user
    - User could also choose public manually

Firewall Profiles in Windows 10



Windows Firewall
Control Panel › System and Security › Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	Network 2
Notification state:	Notify me when Windows Firewall blocks a new app

Guest or public networks — Not connected

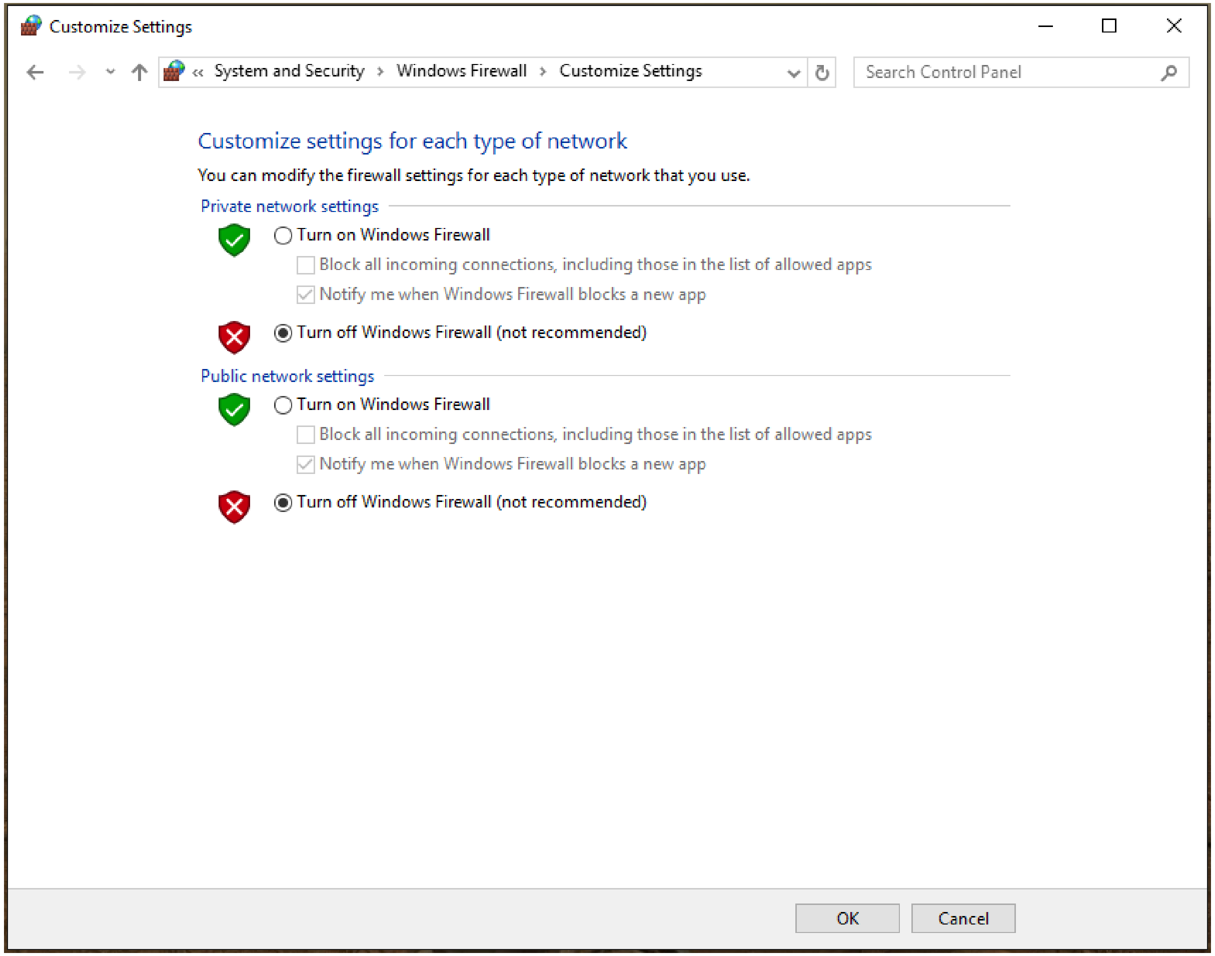
Networks in public places such as airports or coffee shops

Windows Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	None
Notification state:	Notify me when Windows Firewall blocks a new app

Firewall Settings For Labs

- We typically turn the Windows Firewall off for our lab VMs
- This helps with troubleshooting and prevents our test software from failing to connect with the VM
- Unless specified otherwise, turn the Windows Firewall off in your lab VMs

Firewall Settings in Windows 10



Customize Settings
« System and Security › Windows Firewall › Customize Settings
Search Control Panel

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Firewall blocks a new app

● Turn off Windows Firewall (not recommended)

Public network settings

○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Firewall blocks a new app

● Turn off Windows Firewall (not recommended)

Network Access Protection

Network Access Protection

- NAP was created to ensure all the computers connecting to the network are configured properly and have appropriate security measures in place
  - Compares computers against corporate baseline
- Common Checks:
  - Firewall Settings
  - Windows Update turned on and up to date
  - Antivirus Program installed and up to date
  - Local Security Policy Settings

Network Access Protection

- NAP is often used for computers that are accessing the network remotely, or aren't part of the domain (e.g. connecting over a VPN)
  - If a computer is part of the domain, you can control all these setting through GPOs
- When a computer attempts to connect to the network NAP determines if the computer is compliant
  - Computers can either be denied access to the network, or given limited access to the network
    - Limited access to bring their systems in line
      - Getting updates, etc.

Network Access Protection

- The first step in NAP is Health State Validation
  - Seeing if the computer meets NAP requirements
- The second step in NAP is Health Policy Compliance
  - During this step the computer is updated and reconfigured to meet the requirements of NAP
- If the computer still doesn’t meet the NAP requirements the third step could be Limited Access Mode
  - Access can be granted to a portion of the network (updating, downloading AV, etc.)

Network Access Protection

- Enforcement Types
  - IPSec
    - Health state requirements before connecting to IPSec protected hosts
  - 802.1X (wired or wireless)
    - Enables complete control over access to the network(s) based on health state
  - VPN
    - Controlling access from remote clients using a VPN
  - DHCP
    - Only allows compliant computers to get an IP

Network Access Protection

- System Health Agents and Validators
- SHA
  - Runs on the client and validates its health
  - Generates a SoH (statement of health)
  - The SoH is sent to the system health validator
- SHV
  - This is the server component
  - Analyzes the SoH provided by the SHA
  - Generates a SoHR (statement of health response)
    - Used by the policy server to grant access
      - NPS, Network Policy Server

Network Access Protection

- Health Requirement Policies are composed of the following:
  - Connection Request Policy
    - Determines if request needs to be processed
  - System Health Validators
    - Checks the SoH
  - Remediation Server Group
    - Servers clients can connect to, to meet requirements
  - Health Policy
    - Determines the actual health requirements and policies for compliant and non-compliant clients
  - Network Policy
    - Determines network access based on health policy

Homework

- Read about Network Policy & Access Services
  - https://technet.microsoft.com/en-us/network/bb545879.aspx

Lab 07 – NAP

Lab 07 Details

- Before the lab you can run **slmgr /rearm** on both VMs, then reboot them
  - This will save you some time during the lab
  - Should resolve the activation warning messages
- Setting up DHCP
- Setting up NPS
- Configure GPO to force connecting clients to have firewall and automatic updates turned on