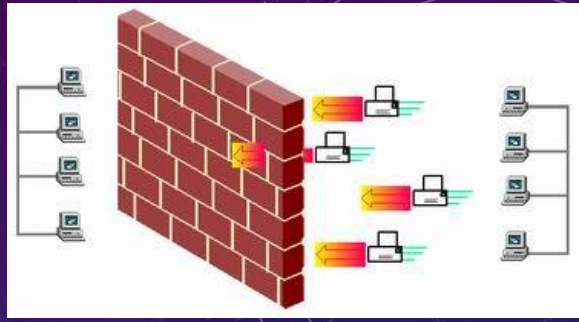
IT2654: SYSTEMS ADMINISTRATION & SECURITY

TOPIC 11: WINDOWS FIREWALL

WINDOWS FIREWALL TOPICS

- What is a firewall?
- Firewall types
- How a firewall works
- Windows firewall features
- Configuring Windows firewall

WHAT IS A FIREWALL?



- A device that filters packets either coming into or going out of a device
- Filtering can be based on IP, TCP, UDP and other criteria relating to a packet as well as authentication.
- Criteria contained in firewall rules.
- Firewall rule is similar to an access control list statement
  - Example: permit host 172.16.1.1 host 180.50.1.1 eq Telnet

WHAT A FIREWALL CAN DO

- A firewall is a focus for security decisions
  - Since all traffic passes through a single checkpoint, security measures can be concentrated on this point
- A firewall can enforce security policy
  - Many internet services are inherently dangerous and firewall can allow or deny such services
- A firewall can log internet activity efficiently
  - Firewall acts as a single point of access for collecting information on the use and misuse of the network
- A firewall limits exposure
  - A firewall can protect the entire network, and a number of firewalls can be deployed to protect individual sub-networks

WHAT A FIREWALL CANNOT DO

- A firewall cannot protect against:
  - Internal network snooping or intrusions
  - Connections that do not pass through it
  - Completely new threats
  - Social Engineering
  - Poorly trained firewall administrator

FIREWALL TYPES

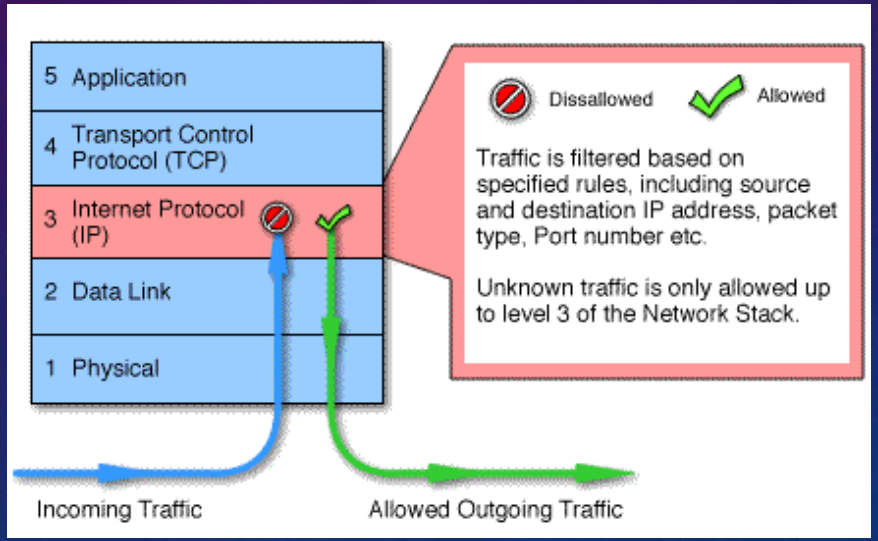
1) **Packet Filtering**
   - Packet filtering makes each filtering decision on a packet by packet basis without regard to previous packets in any direction.
2) **Stateful Packet Inspection (SPI)**
   - Stateful firewall keeps track of packet flows and filters based on flow information
3) **Proxy Server**
   - Proxy firewall works on a per-application basis. User sends to proxy, proxy creates new packet sourced from proxy

FIREWALL TYPES

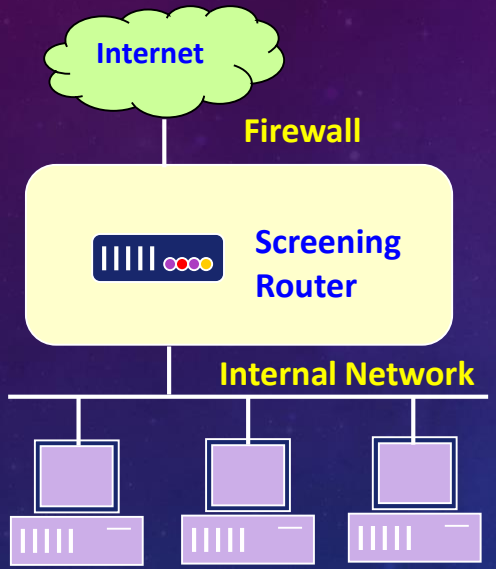
- Network-based vs host-based
  - Network-based runs a router, multi-layer switch or dedicated firewall
  - Host-based firewall runs on computer running OS such as Windows or UNIX
- Hardware vs software firewall
  - Hardware firewall chassis designed for specifically to operate as a firewall; highest performance

PACKET FILTERING FIREWALL

- Provides network-layer security to control the types of information sent between networks and hosts.



HOW PACKET FILTERING WORKS



- Inspect the IP header
- Apply the values against the filtering and access rules
- Decide whether to route (permit) or not to route (deny) the packet
- The decision is based on the security policy configured

TYPES OF PACKET FILTERING

- Filtering by address
  - Example source, destination addresses
- Filtering by protocol
  - Example TCP, UDP, ICMP
- Filtering by services
  - Based on well known port number
  - Example port number 80 for HTTP

NETWORKING PORT

- In TCP/IP and UDP networks, a *port* is an endpoint to a logical connection. The port number identifies what type of port it is.

- The three categories of TCP and UDP ports are:
  1) Well known ports – 0 to 1023
     example – HTTP (80)
  2) Registered ports - 1,024 to 49,151
     example – Microsoft RDP (3389)
  3) Dynamic or private ports - 49,152 to 65,535

WELL-KNOWN PORT NUMBERS

Port	Primary Protocol*	Application
20	TCP	FTP Data Traffic
21	TCP	FTP Supervisory Connection
22	TCP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol (SMTP)
53	UDP	Domain Name System (DNS)

WELL-KNOWN PORT NUMBERS

Port	Primary Protocol	Application
69	UDP	Trivial File Transfer Protocol (TFTP)
80	TCP	Hypertext Transfer Protocol (HTTP)
110	TCP	Post Office Protocol (POP)
135-139	TCP	NETBIOS service for peer-to-peer file sharing in older versions of Windows
143	TCP	Internet Message Access Protocol (IMAP)
161	UDP	Simple Network Management Protocol (SNMP)
443	TCP	HTTP over SSL/TLS

FILTERING RULES

Rule	Direction	Source Address	Destination Address	Protocol	Source Port	Destination Port	Action
1	Out	Internal	Any	TCP	>1023	23	Permit
2	In	Any	Internal	TCP	23	>1023	Permit
3	Any	Any	Any	Any	Any	Any	Deny

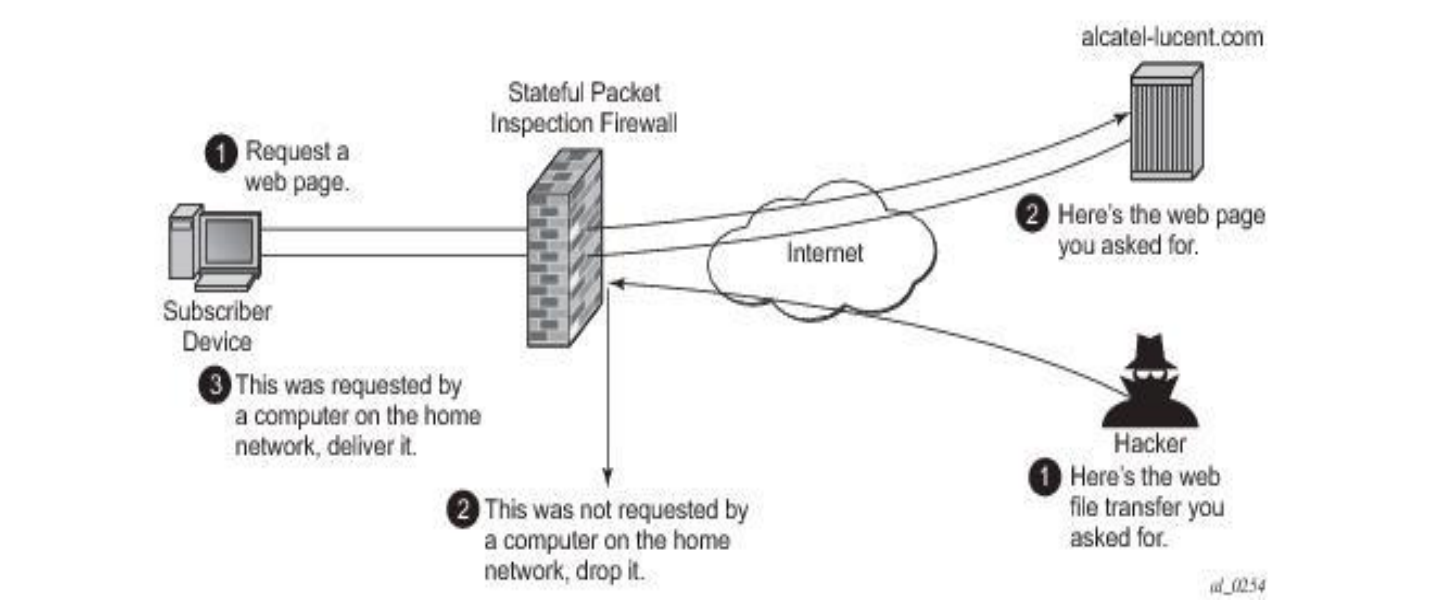
- Filtering rules are applied to the packet in order. The first matching condition is the rule applied to the packet.
- For safety, filtering rules should have a deny all condition at the end of the rules.

EXAMPLE - FILTERING TELNET

Rule	Direction	Source Address	Destination Address	Protocol	Source Port	Destination Port	Action
1	Out	Internal	Any	TCP	>1023	23	Permit
2	In	Any	Internal	TCP	23	>1023	Permit
3	Any	Any	Any	Any	Any	Any	Deny

- Rule 1 - allows outgoing Telnet (port 23)
- Rule 2 - allows response from Telnet server
- Rule 3 - is the default deny rule

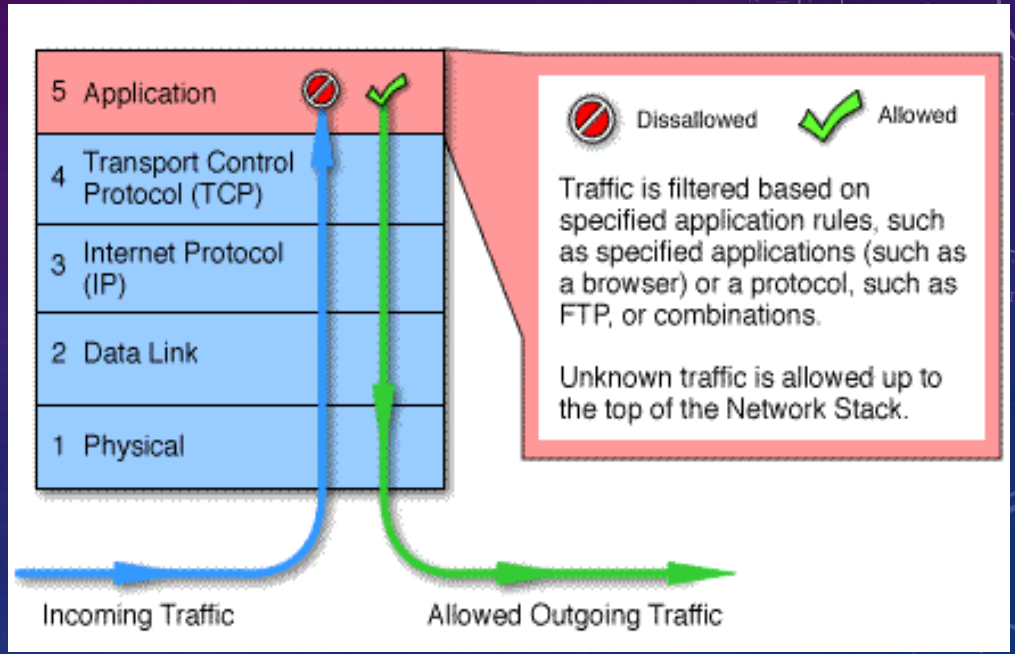
STATEFUL PACKET INSPECTION (SPI)



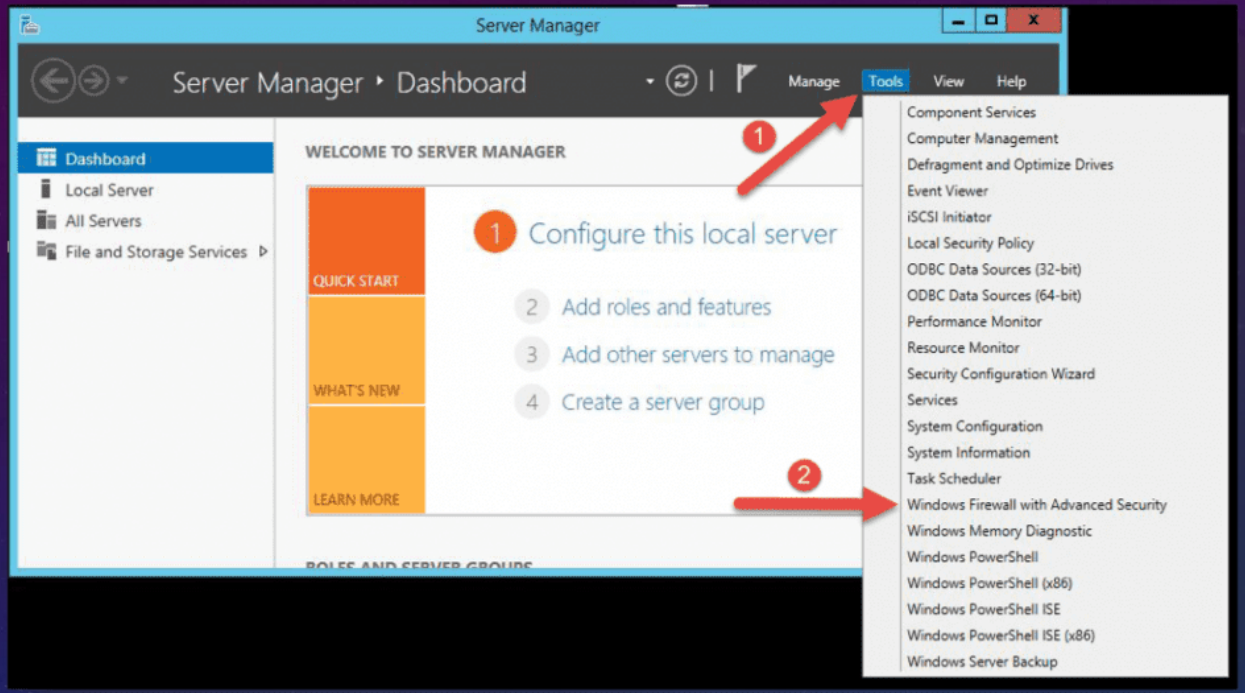
A firewall with stateful packet inspection looks at packets in groups rather than individually. It keeps track of which packets have passed through the firewall and can detect patterns that indicate unauthorized access.

PROXY SERVER OR APPLICATION FIREWALLS

- Also called Proxy Services
- Filter packets at the application layer
- A proxy server acts as a gateway between you and the internet. It's an intermediary server separating end users from the websites they browse.



WINDOWS FIREWALL



- by default, allows all *outbound* connections, and permits only *established inbound* connections
- deny all other inbound traffic

WINDOWS FIREWALL FEATURES

- Inbound filtering
- Outbound filtering
- Firewall rules combined with IPsec rules
- Support for logging

LOCATIONS AND THE FIREWALL

- Windows Firewall with Advanced Security is a network location aware application
- Windows stores the firewall properties based on location types
- Configuration for each location type is called a profile
- Profiles are simply a grouping of firewall rules dependent on where a server is connected.
- In each profile you can:
    - Enable or disable Windows Firewall
    - Configure inbound and/or outbound connections
    - Customize logging and other settings

WINDOWS FIREWALL PROFILES

WINDOWS FIREWALL PROFILES

1) **Domain Profile**

- used when a computer connects to the corporate network.
- device can detect the domain controller.
- Should be the least restrictive because security is usually very well controlled.

2) **Private Profile**

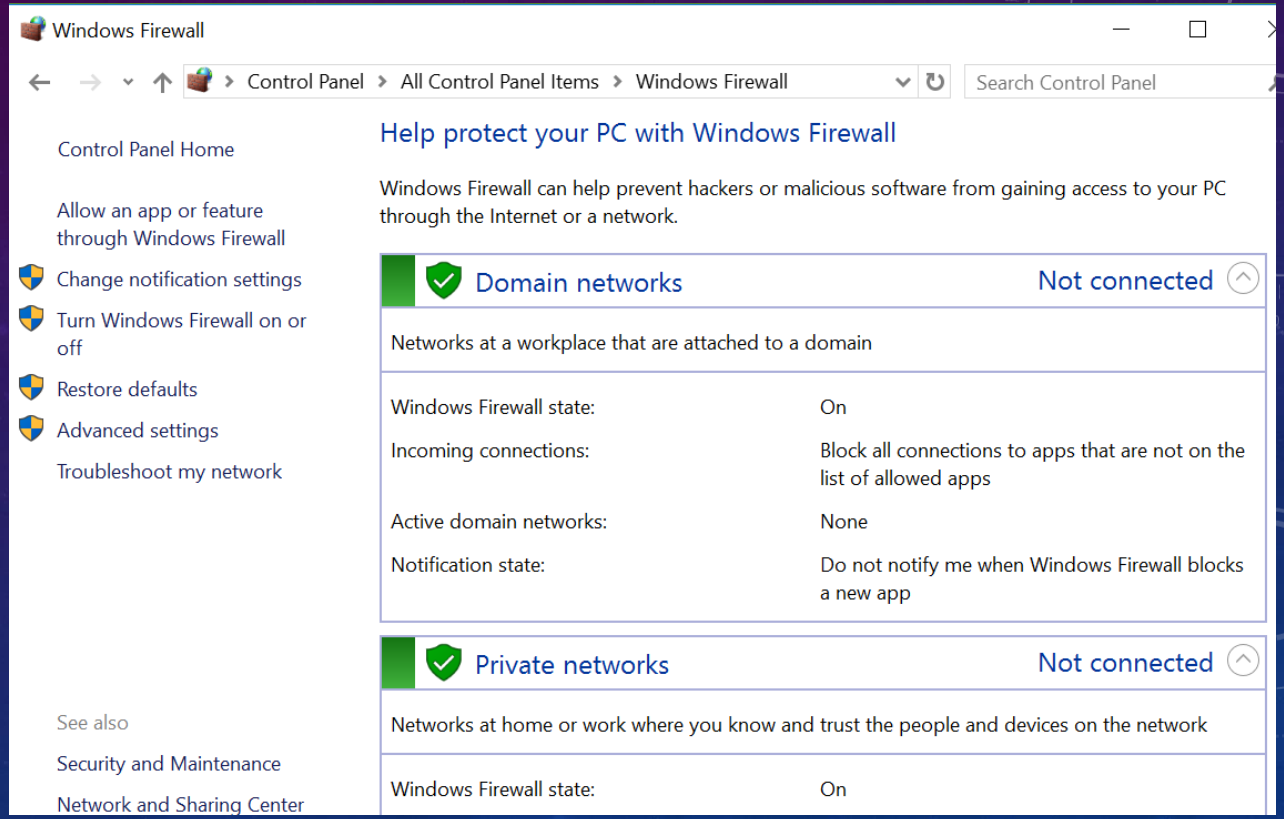
- computers that connect to a private network, such as home or office. In private networks, users are not directly exposed to the Internet.
- Less restrictive than domain profile.

3) **Public Profile**:

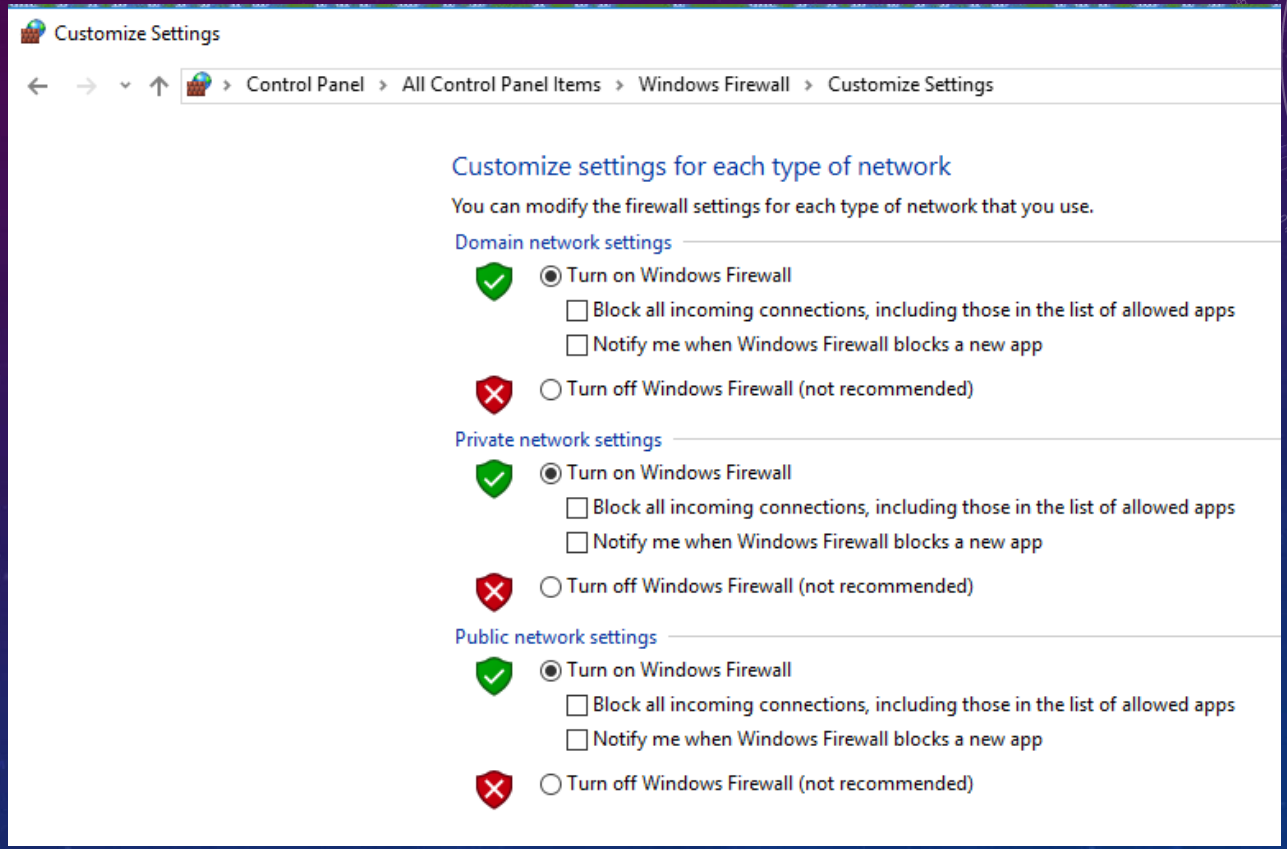
- used when computer is connected directly to a public network like a restaurant, library or airport.
- Should be the most restrictive because the network is least secured.

CONFIGURING WINDOWS FIREWALL

- Control Panel – Windows Firewall



BASIC FIREWALL CONFIGURATION



ADVANCED FIREWALL CONFIGURATION

- Firewall → Advanced settings
- Run from Server Manager
- wf.msc command
- Allows you to configure more complex rules, outgoing filtering, and IPsec rules

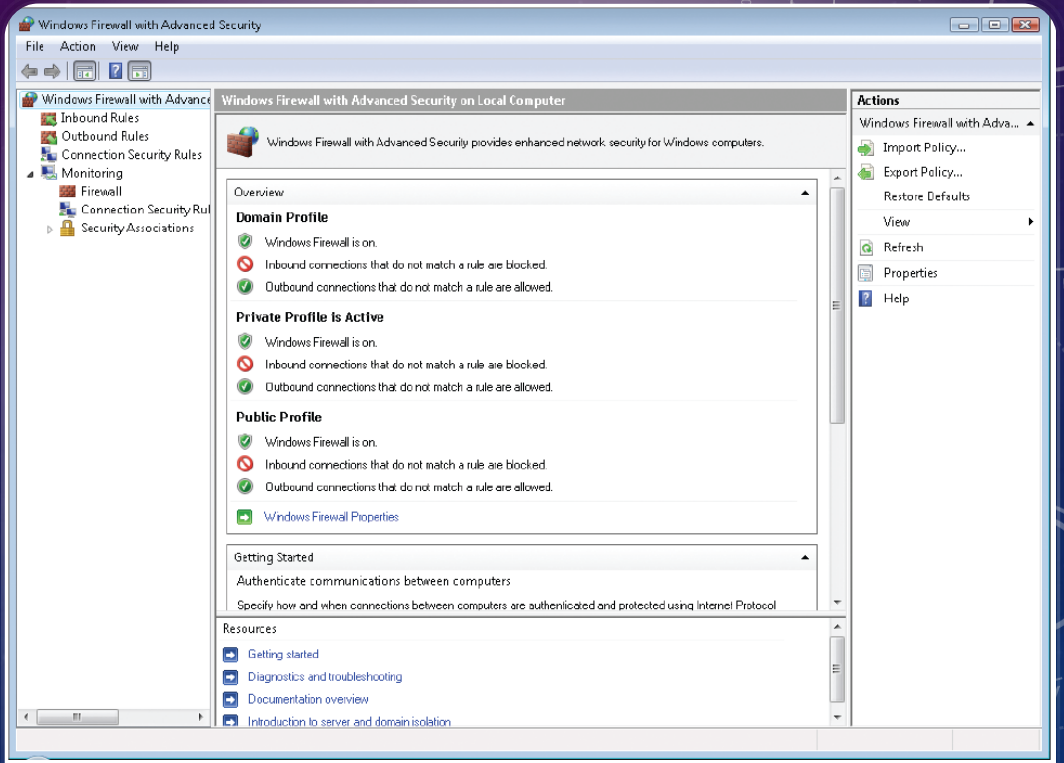
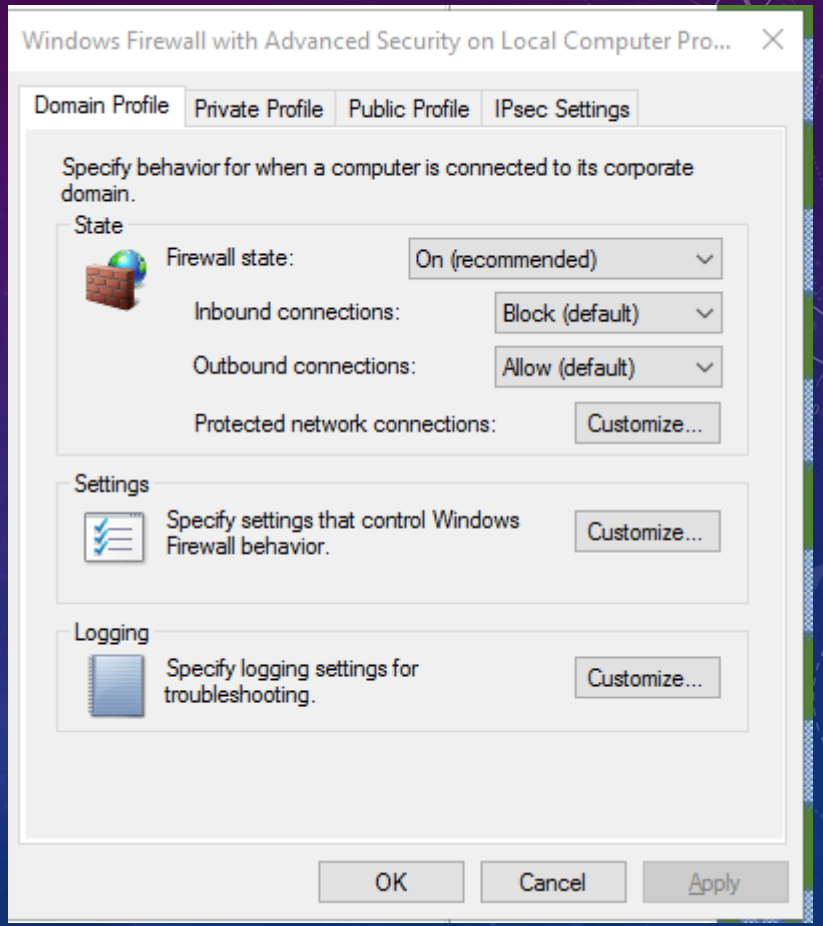


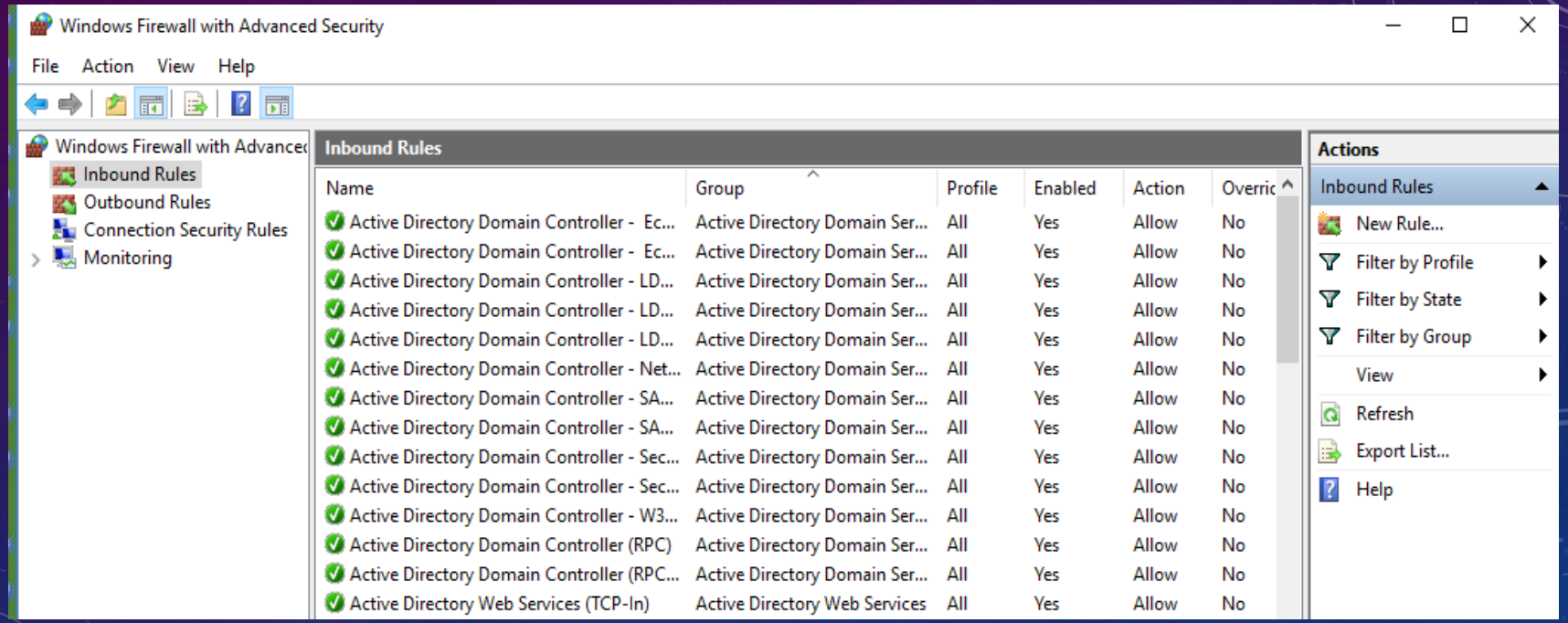
Figure 8-21 Windows Firewall and Advanced Security snap-in

WINDOWS FIREWALL WITH ADVANCED SECURITY - PROPERTIES

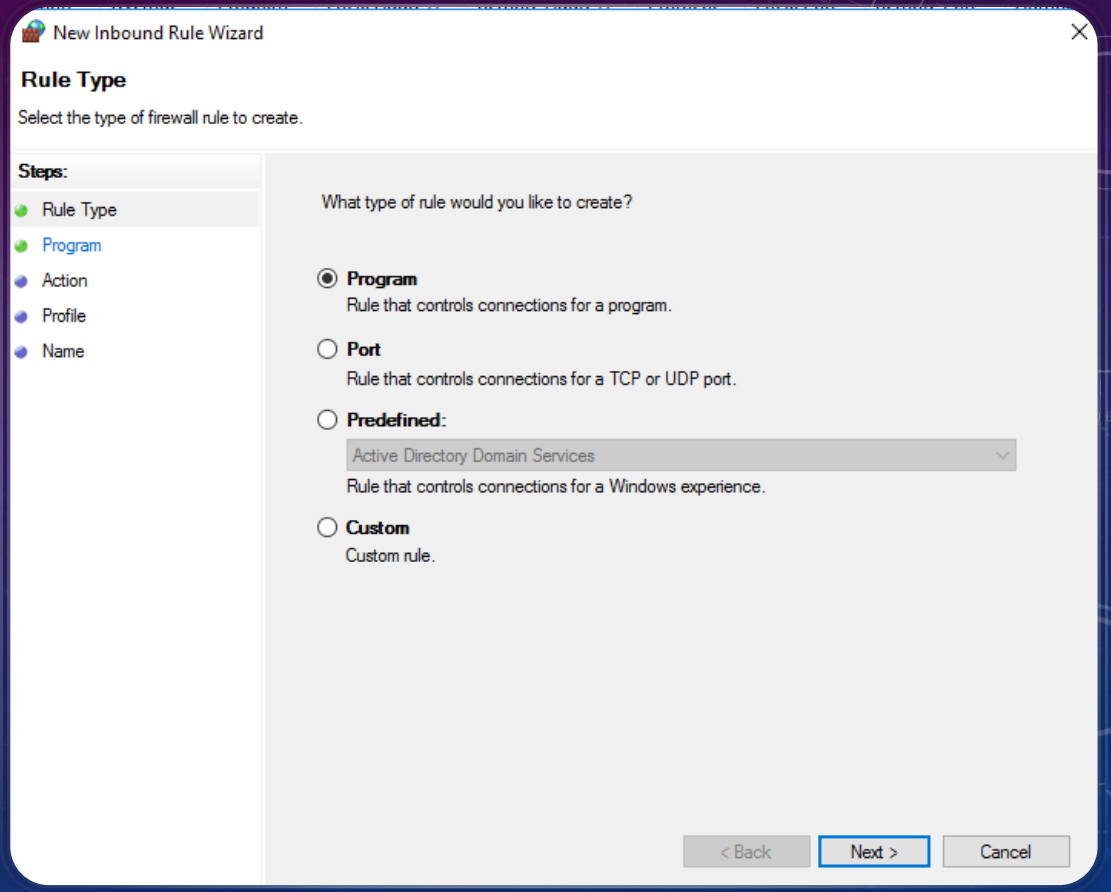
IPSec allows data to be encrypted as it is transmitted across the network.



INBOUND RULES



NEW INBOUND RULE WIZARD



OUTBOUND RULES

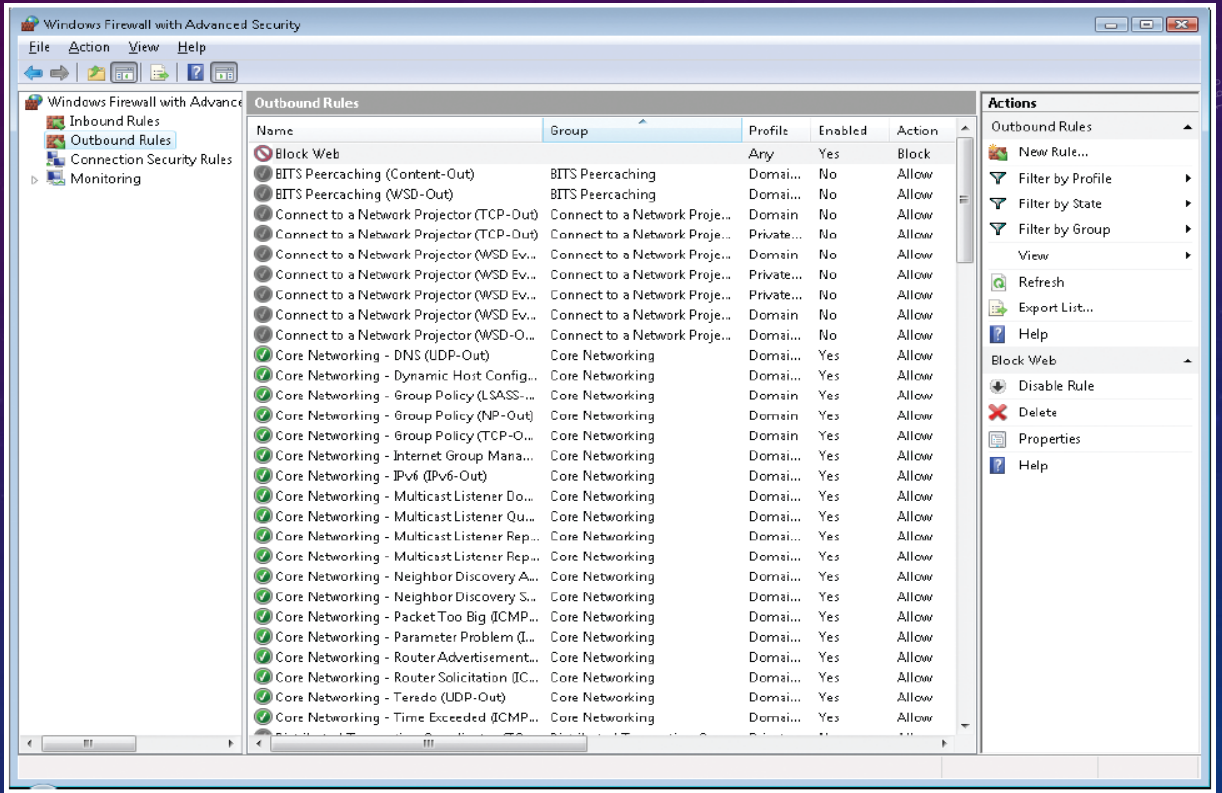


Figure 8-24 Outbound Rules

NEW OUTBOUND RULE WIZARD

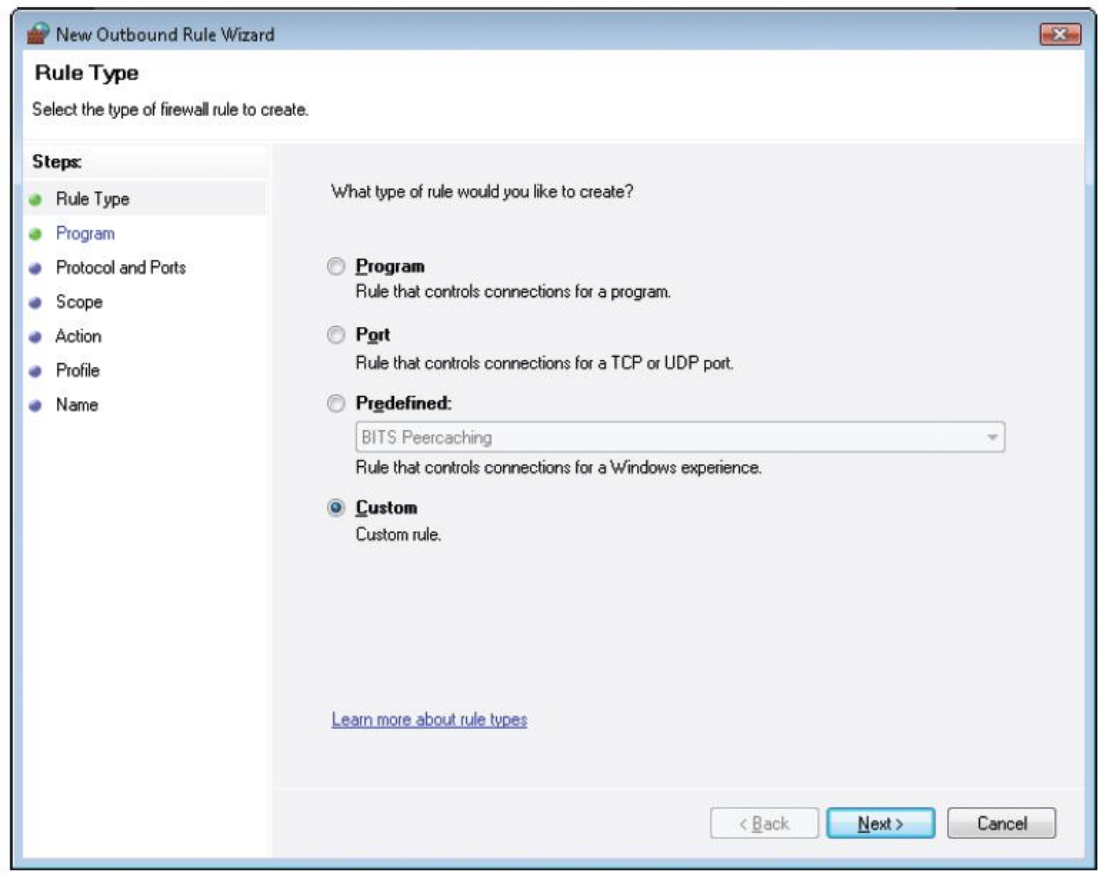


Figure 8-26 New Outbound Rule Wizard, Rule Type selection

CONNECTION SECURITY RULES

- Specify how and when Windows Firewall with Advanced Security uses IPsec to protect traffic passing between the local computer and other computers on the network.
- Force two peer computers to authenticate before a connection can be established between them.
- Ensure that communications between the computers is secure by encrypting all traffic passed between them

SUMMARY

- What is a firewall?
- Types of firewalls
- Networking ports
- Windows firewall
- features
- firewall profiles
- configuration