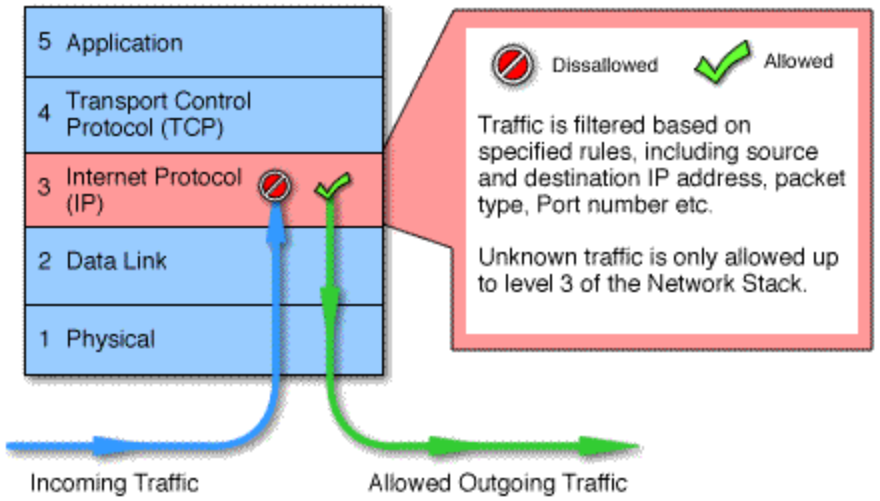
Computer Networ
Firewa

Firewalls

1. Four major types of firewalls in OSI
2. Window firewalls
3. Router firewalls
4. Firewalls design

Four major types of firewalls in OSI

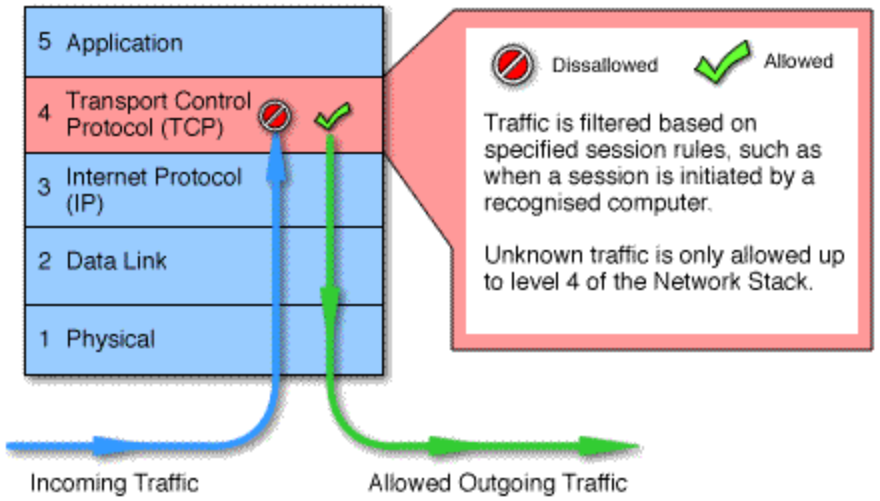


GO BACK

Four major types of firewalls in OSI

- Packet filters –
- work at the network level.
- compared to a set of criteria before it is forwarded
- Advantages: low cost, low impact on network performance.
- Disadvantages: does not support sophisticated rule based models.

Four major types of firewalls in OSI



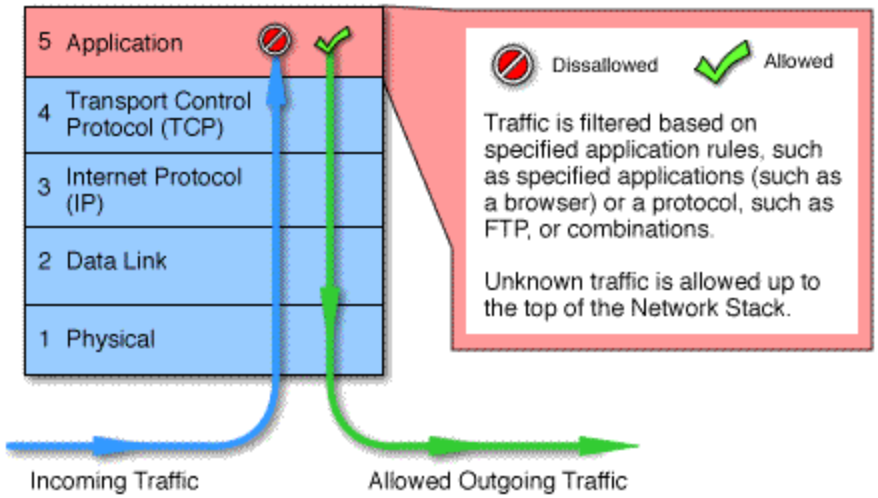
GO BACK

Four major types of firewalls in OSI

- Circuit level gateways
- work at the session layer
- monitor TCP handshaking between packets to determine whether a requested session is legitimate
- Information passed to remote computer through a circuit level gateway appears to have originated from the gateway.
- Advantages: relatively inexpensive , hiding information about the private network Disadvantages: they do not filter individual packets.

GO BACK

Four major types of firewalls in OSI



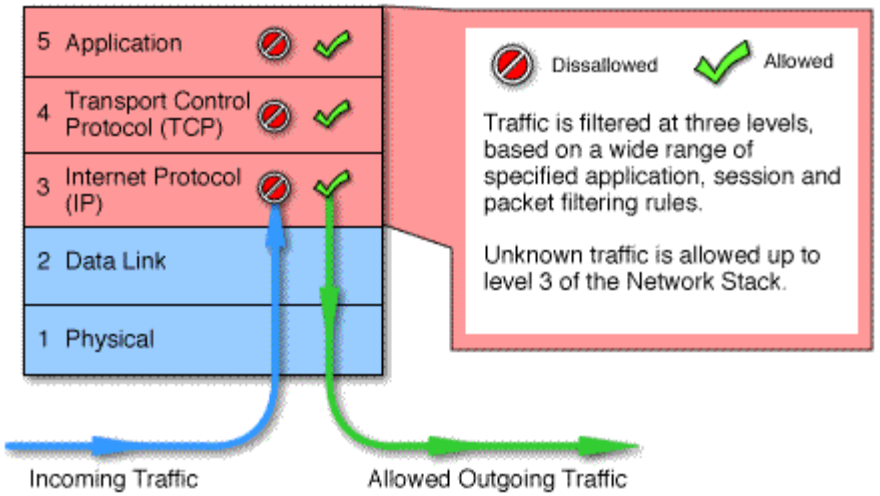
GO BACK

Four major types of firewalls in OSI

- Application level gateways
- work at the application layer
- Incoming or outgoing packets cannot access services for which there is no proxy
- filter application specific commands
- can also be used to log user activity and logins.
- Advantages: a high level of security
- Disadvantages: having a significant impact on network performance, not transparent to end users and require manual configuration of each client computer.

GO BACK

Four major types of firewalls in OSI



GO BACK

Four major types of firewalls in OSI

- Stateful multilayer inspection firewalls
- work at the application , session, network layer.
- They filter packets at the network layer, determine whether session packets are legitimate and evaluate contents of packets at the application layer
- They allow direct connection between client and host, alleviating the problem caused by the lack of transparency of application level gateways. can also be used to log user activity and logins.
- They rely on algorithms to recognize and process application layer data instead of running application specific proxies.
- Advantages: a high level of security, good performance, transparency to end users
- Disadvantages: they are expensive and complex.

What is Windows Firewall

- In 2003, Sasser worm and blaster worm attacked a large number of Windows machines, taking advantage of flaws in the RPC Windows service. Adding to that, Microsoft was criticized for not being active in protecting customers from threats. Therefore, Microsoft decided to improve both functionality and the interface of Windows XP's built-in firewall, and rebrand it as: "Windows Firewall".

GO BACK

What is Windows Firewall?

- Windows Firewall helps protecting your computer by preventing unauthorized users from gaining access to your computer through a network or internet.

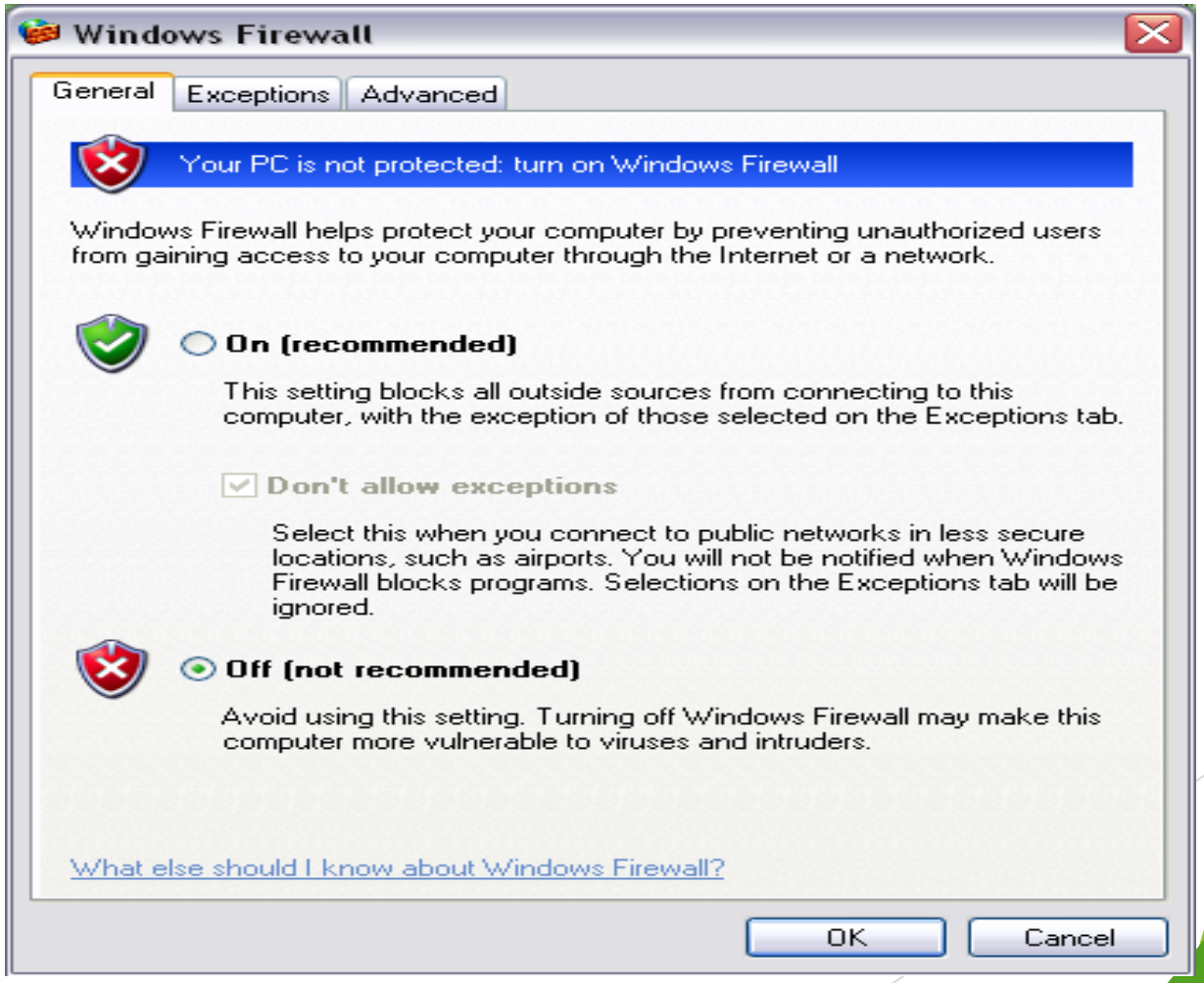
GO BACK

What does it do

- Help block computer viruses and worms from reaching your computer.
- Ask for your permission to block or unblock certain connection requests.
- Create a record (a security log)

GO BACK

What does it do



GO BACK

Router Firewall

- Hardware firewall
- Difference between Hardware firewall and Software firewall:
- Configuring for maximum security
- Strengthening Home router firewalls
- Block ICMP traffic, or 'stealth' mode:
- Stateful packet inspection:
- Disable remote administration
- Attack detection:
- Disable file and printer sharing

GO BACK

Router Firewall

- Hardware firewall
- Difference between Hardware firewall and Software firewall:
- Configuring for maximum security
- Strengthening Home router firewalls
- Block ICMP traffic, or 'stealth' mode:
- Stateful packet inspection:
- Disable remote administration
- Attack detection:
- Disable file and printer sharing

GO BACK

Router Firewall

- Allowing common applications through Home Internet sharing devices
- Hosting websites, games and FTP behind your firewall
- Monitoring your firewall (optional)

GO BACK

Firewall design

- Problems you will encounter when using a firewall
-
- · Unknown applications
- · Application functionality not understood
- · Applications tunneled in another protocol, like HTTP, and not visible to firewall
- · Firewall clients incompatible with certain applications
- · Features, like authentication, not supported
- · Getting certain applications to work behind firewall can be troublesome
- · Firewall failure & high availability
- · Firewall bugs
- · False sense of security - remember the multi-layer (defense in depth) approach
-

GO BACK

Firewall design

- Benefits to using a firewall
-
- · Protect your network or PC
- · Prevent viruses and worms on your network
- · Prevent malicious attackers from getting into your network
- · Prevent ad-ware, malware, and spyware
- · Prevent loss of sensitive or valuable company information
- · Prevent Denial of Service (DoS) attacks
- · Acting as a forensics tool
- · Authenticate users, log users (accounting), and authorize users only for certain content or applications

Firewall design

- How many firewalls do I need, what kind, and where do I put them?
- · Good question
- · Multiple design scenarios are available
- · Minimally, one at the Internet edge
- · Additionally, here are some other models:
- o Two firewalls with DMZ in the middle
- o Firewall at backbone edge
- o Firewall at edge of each department
- o Firewall between companies
- o Firewall between corporate and remote locations
- o Software firewall on each client PC
- · What kind of firewall is needed is also a good question. Vendors differ. In general, a SPI network firewall that provides the features you need is the minimum.

Firewall design

- Choosing the right firewall
-
- · Costs - not just initial purchase but cost of add-ins, support, learning curve, and maintenance (TCO).
- · Hardware specifications-
- o CPU, RAM, Disk
- o Scalability
- o Extensibility
- o Reliability
- o High Availability
- o Load balancing
- o Compatibility
- o Ease of use
- o Vendor support
- · Firewall features-
- o AAA

GO BACK

Firewall design

- Implementing a new firewall
-
- · Compare firewalls and evaluate in house. Don't believe what vendors tell you, test it for yourself.
- · If unfamiliar with the model selected, have an experienced consultant configure the new firewall and implement.
- · Before implementing, make sure that thorough testing is performed. Firewall configurations can be tricky and the slightest error in configuration can cause no traffic to flow.
- · Have a fail back plan in case the new firewall doesn't work as expected.
- · Make sure that firewalls "fail shut", meaning if the firewall doesn't work, you never want a situation where all inbound access is allowed. If even seconds pass where a company doesn't have a firewall, there can be very bad consequences.
- · Remember the defense in depth approach - the firewall isn't the single cure-all for security.

Firewall design

- Introduction to ISA Server Concepts
-
- · Part of defense in depth / security in layers
- · Securing your network is a continual process
- · Used to secure the perimeter of your network - which can be difficult to define
- · ISA is a firewall
- · To do this, ISA uses:
- o packet filtering
- o stateful filtering
- o and application-layer filtering
- · Application-layer filtering is unique

Firewall design

- Overview of ISA Features
-
- · ISA provides secure Internet access - per user, per website, per protocol, log all requests, and no direct connection to the Internet by the client
- · ISA allows you to securely publish internal resources with application content filters - SMTP app filter, SMTP screener, OWA/OMA app filter, etc.
- · ISA provides VPN access - remote access VPN and site-to-site
- · ISA provides web caching
- · ISA offers basic IDS detection
- · Numerous ISA add-ins are available

Firewall design

- Initial Configuration of ISA Server
-
- · Numerous deployment scenarios
- · No traffic is allowed, by default
- · Common initial tasks are:
- o Create networks
- o Create firewall policies
- o Define web caching policies
- o Configure VPN access
- o Enable client connection methods

Firewall design

- Management of ISA Server
-
- · Use ISA server management console (MMC)
- · ISA server performance monitor is available
- · ISA management console is broken down into:
- o Monitoring
- o Firewall Policy
- o Virtual Private Networks
- o Configuration
- · Networks
- · Cache
- · Add-ins
- · General

GO BACK

Firewall design

- What ISA does and what it doesn’t do
- <u>ISA Does:</u>
- · Stateful Packet Inspection (SPI) firewall protection
- · Proxy
- · Integrated Windows authentication
- · Logging
- · Reporting and analysis
- · Caching
- · VPN - site to site and remote client access
- · Basic IDS
- <u>ISA Doesn't:</u>
- · Scan for viruses, worms, spyware, adware, or malware
- · Provide a high level of intrusion detection and prevention
- · Provide in-depth reporting and analysis of usage logs

Thank You !