

# Firewalls

# Outline

- What are firewalls?
- Types of Firewalls
- Building a simple firewall using Netfilter
- Iptables firewall in Linux
- Stateful Firewall
- Application Firewall
- Evading Firewalls

# Firewalls

- A part of computer system or network designed to stop unauthorized traffic flowing from one network to another.
- Separate trusted and untrusted components of a network.
- Differentiate networks within a trusted network.
- Main functionalities are filtering data, redirecting traffic and protecting against network attacks.

# Requirements of a firewall

- All the traffic between trust zones should pass through firewall.
- Only authorized traffic, as defined by the security policy, should be allowed to pass through.
- The firewall itself must be immune to penetration, which implies using a hardened system with secured Operating Systems.

# Firewall Policy

- User control: Controls access to the data based on the role of the user who is attempting to access it. Applied to users inside the firewall perimeter.
- Service control: Controls access by the type of service offered by the host. Applied on the basis of network address, protocol of connection and port numbers.
- Direction control: Determines the direction in which requests may be initiated and are allowed to flow through the firewall. It tells whether the traffic is “inbound” (From the network to firewall) or vice-versa “outbound”

# Firewall actions

Accepted: Allowed to enter the connected network/host through the firewall.

Denied: Not permitted to enter the other side of firewall.

Rejected: Similar to “Denied”, but tells the source about this decision through ICMP packet.

*Ingress filtering: Inspects the incoming traffic to safeguard an internal network and prevent attacks from outside.*

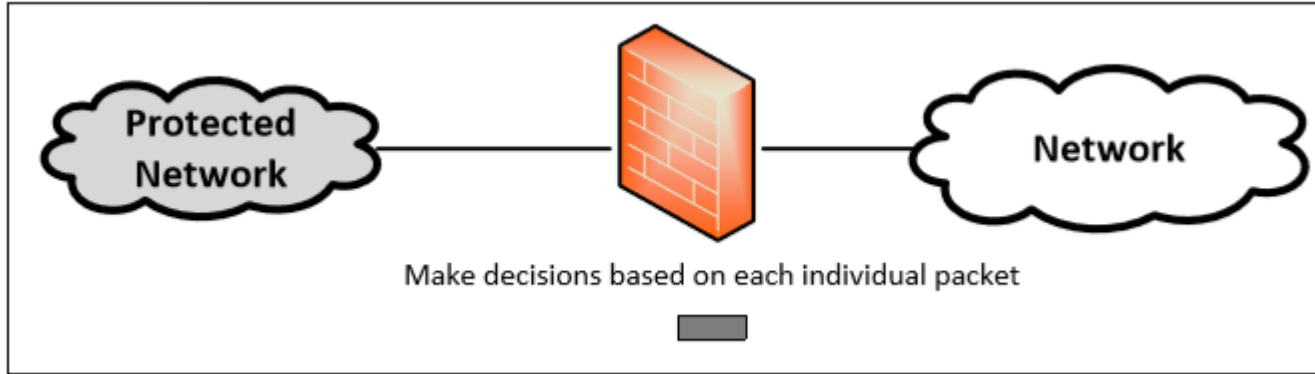
*Egress filtering: Inspects the outgoing network traffic and prevent the users in the internal network to reach out to the outside network. For example like blocking social networking sites etc.*

# Types of filters

Depending on the mode of operation, there are three types of firewalls :

- Packet Filter Firewall
- Stateful Firewall
- Application/Proxy Firewall

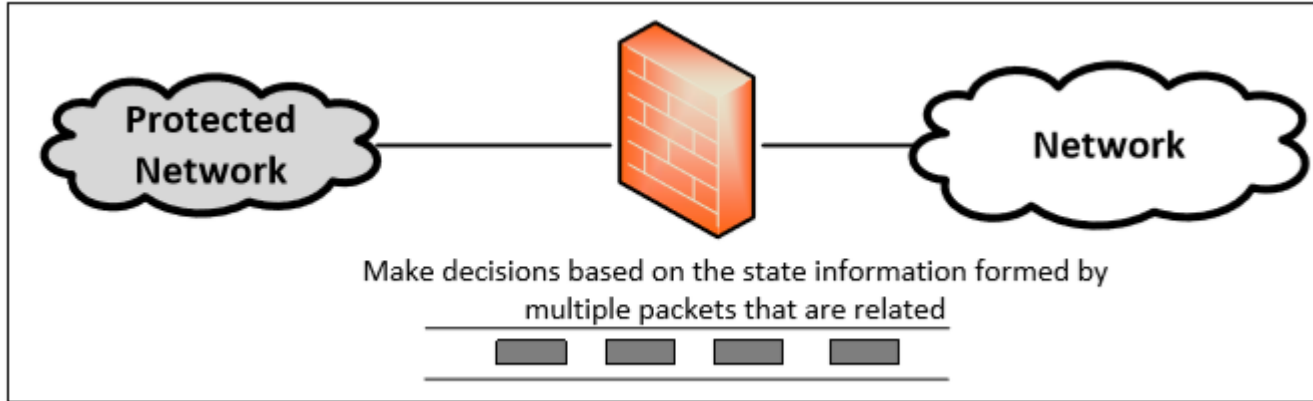
# Packet Filter Firewall



- Doesn't pay attention to if the packet is a part of existing stream or traffic.
  - Doesn't maintain the states about packets. Also called Stateless Firewall.
- Controls traffic based on the information in packet headers, without looking into the payload that contains application data.



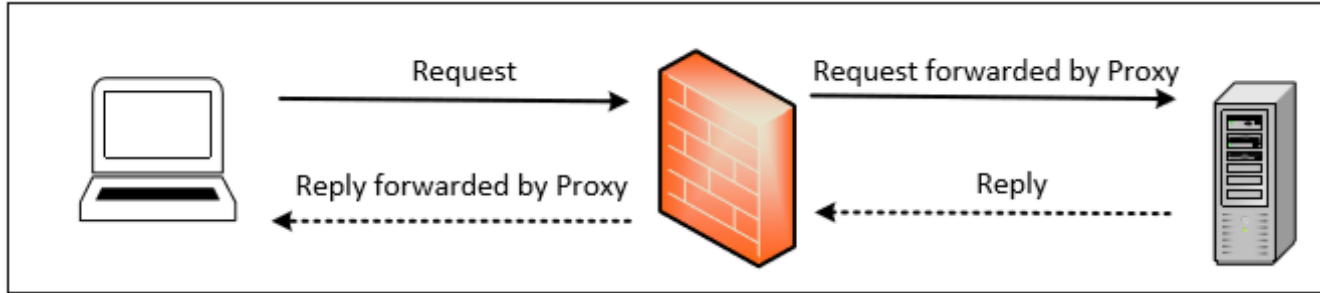
# Stateful Firewall



- Example : Connections are only allowed through the ports that hold open connections.

- Tracks the state of traffic by monitoring all the connection interactions until is closed.
- Connection state table is maintained to understand the context of packets.

# Application/Proxy Firewall



- Controls input, output and access from/to an application or service.
- The client's connection terminates at the proxy and a separate connection is initiated from the proxy to the destination host.
- Data on the connection is analyzed up to the application layer to determine if the packet should be allowed or rejected.
- Acts as an intermediary by impersonating the intended recipient.

# Iptables Firewall in Linux

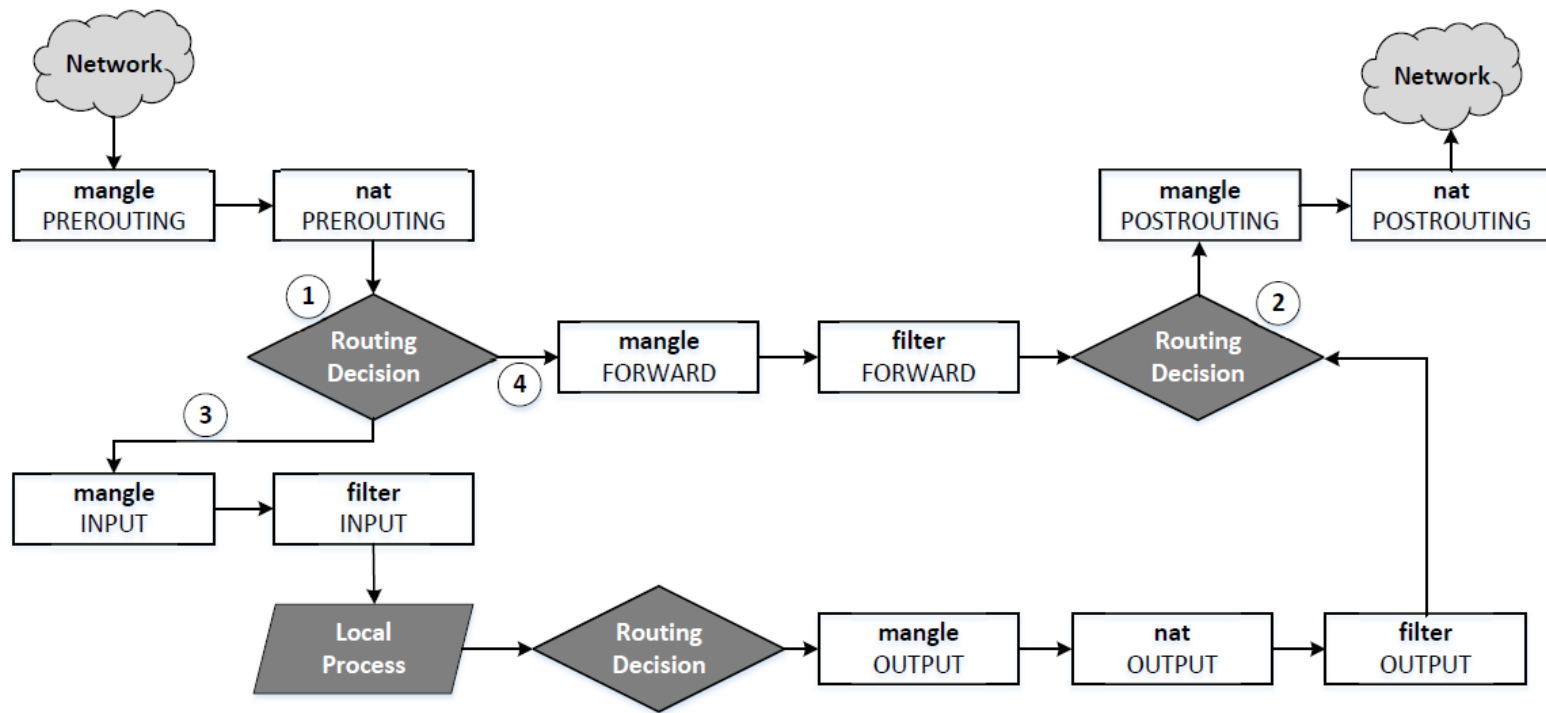
- Iptables is a built-in firewall based on netfilter.
- Kernel part: Xtables
- User-space program: iptables
- Usually, iptables refer to both kernel and user space programs.
- Rules are arranged in hierarchical structure as shown in the table.

| Table  | Chain   | Functionality                                     |
|--------|---|---|
| filter | INPUT<br>FORWARD<br>OUTPUT                              | Packet filtering                                  |
| nat    | PREROUTING<br>INPUT<br>OUTPUT<br>POSTROUTING            | Modifying source or destination network addresses |
| mangle | PREROUTING<br>INPUT<br>FORWARD<br>OUTPUT<br>POSTROUTING | Packet content modification                       |

# Iptables Firewall - Structure

- Each table contains several chains, each of which corresponds to a netfilter hook.
- Each chain indicates where its rules are enforced.
  - Example : Rules on FORWARD chain are enforced at `NF_IP_FORWARD` hook and rules on INPUT chain are enforced at `NF_IP_LOCAL_IN` hook.
- Each chain contains a set of firewall rules that will be enforced.
- User can add rules to the chains.
  - Example : To block all incoming telnet traffic, add a rule to the INPUT chain of the filter table

# Traversing Chains and Rule Matching



# Traversing Chains and Rule Matching

- 1 - Decides if the final destination of the packet is the local machine
- 3 - Packet traverses through INPUT chains
- 4 - Packet traverses through FORWARD chains
- 2 - Decides from which of the network interface to send out outgoing packets

As a packet traverses through each chain, rules on the chain are examined to see whether there is a match or not. If there is a match, the corresponding target action is executed: ACCEPT, DROP or jumping to user-defined chain.

# Traversing Chains and Rule Matching

Example: Increase the TTL field of all packets by 5.

Solution: Add a rule to the mangle table and choose a chain provided by netfilter hooks. We choose PREROUTING chain so the changes can be applied to all packets, regardless they are for the current host or for others.

```
// -t mangle = Add this to 'mangle' table  
// -A PREROUTING = Append this rule to PREROUTING chain  
  
iptables -t mangle -A PREROUTING -j TTL --ttl-inc 5
```

# Iptables Extension

Iptables functions can be extended using modules also called as extensions.

Two Examples:

Conntrack: To specify rules based on connections to build stateful firewalls.

Owner: To specify rules based on user ids. Ex: To prevent user Alice from sending out telnet packets. Owner module can match packets based on the user/group id of the process that created them. This works only for OUTPUT chain (outgoing packets) as it is impossible to find the user ids for INPUT chain (incoming packets).



# Iptables Extension: Block a Specific User

```
seed$ sudo iptables -A OUTPUT -m owner --uid-owner seed -j DROP
seed$ telnet 10.0.2.5
Trying 10.0.2.5...
telnet: Unable to connect to remote host: ... ← telnet is blocked!

seed$ su bob
Password:
bob$ telnet 10.0.2.5
Trying 10.0.2.5...
Connected to 10.0.2.5.
Escape character is '^]'.
Ubuntu 12.04.2 LTS
ubuntu login: ← telnet works!
```

This rule drops the packets generated by any program owned by user seed. Other users are not affected.

# Building a Simple Firewall

- Flush all existing firewall configurations
- Default policy is set to ACCEPT before all the rules.

```
// Set up all the default policies to ACCEPT packets.  
$ sudo iptables -P INPUT ACCEPT  
$ sudo iptables -P OUTPUT ACCEPT  
$ sudo iptables -P FORWARD ACCEPT  
  
// Flush all existing configurations.  
$ sudo iptables -F
```

# Building a Simple Firewall

- Rule on INPUT chain to allow TCP traffic to ports 22 and 80

```
// Allow all incoming TCP packets bound to destination port 22.  
// -A INPUT: Append to existing INPUT chain rules.  
// -p tcp: Select TCP packets  
// -dport 22: Select packets with destination port 22.  
// -j ACCEPT: Accept all the packets that are selected.  
$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT  
  
// Similarly, accept all packets bound to destination port 80.  
$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

- Rule on OUTPUT chain to allow all outgoing TCP traffic

```
// Allow all outgoing TCP traffic.  
// -A OUTPUT: Append to existing OUTPUT chain rules.  
// -p tcp: Apply on TCP protocol packets  
// -m tcp: Further apply matching rules defined in 'tcp' module.  
// -j ACCEPT: Let the selected packets through.  
  
$ sudo iptables -A OUTPUT -p tcp -m tcp -j ACCEPT
```

# Building a Simple Firewall

- Allow the use of the loopback interface.

```
// -I INPUT 1 : Insert a rule in the 1st position of the INPUT chain.  
// -i lo : Select packets bound for the loopback (lo) interface.  
// -j ACCEPT: Accept all the packets that are selected.  
  
$ sudo iptables -I INPUT 1 -i lo -j ACCEPT
```

- Allow DNS queries and replies to pass through.

```
// Allow DNS queries and replies to pass through.  
  
$ sudo iptables -A OUTPUT -p udp --dport 53 -j ACCEPT  
$ sudo iptables -A INPUT -p udp --sport 53 -j ACCEPT
```


# Building a Simple Firewall

```
seed@ubuntu:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination
ACCEPT     tcp  --  anywhere               anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere               anywhere             tcp dpt:http
ACCEPT     udp  --  anywhere               anywhere             udp spt:domain


Chain FORWARD (policy DROP)
target     prot opt source                destination

Chain OUTPUT (policy DROP)
target     prot opt source                destination
ACCEPT     tcp  --  anywhere               anywhere             tcp
ACCEPT     udp  --  anywhere               anywhere             udp dpt:domain

// Setting default filter policy to DROP.
$ sudo iptables -P INPUT DROP
$ sudo iptables -P OUTPUT DROP
$ sudo iptables -P FORWARD DROP
```



These are all the rules we have added



Change the default policy to DROP so that only our configurations on firewall work.

# Building a Simple Firewall: Testing

```
$ telnet 10.0.2.6      ← Our firewall is running on 10.0.2.6.  
Trying 10.0.2.6...  
telnet: Unable to connect to remote host: ...      ← Blocked!  
$ wget 10.0.2.6  
--2017-01-25 18:31:41-- http://10.0.2.6/  
Connecting to 10.0.2.6:80... connected.  
HTTP request sent, awaiting response... 200 OK      ← Succeeded!
```

- To test our firewall, make connection attempts from a different machine.
- Firewall drops all packets except the ones on ports 80(http) and 22(ssh).
- Telnet connection made on port 23 failed to connect, but wget connection on port 80 succeeded.

# Stateful Firewall using Connection Tracking

- A stateful firewall monitors incoming and outgoing packets over a period of time.
- Records attributes like IP address, port numbers, sequence numbers. Collectively known as connection states.
- A connection state, in context of a firewall signifies whether a given packet is a part of an existing flow or not.
- Hence, it is applied to both connection-oriented (TCP) and connectionless protocols (UDP and ICMP).

# Connection Tracking Framework in Linux

- `nf_conntrack` is a connection tracking framework in Linux kernel built on the top of netfilter.
- Each incoming packet is marked with a connection state as described:
  - **NEW**: The connection is starting and packet is a part of a valid sequence. It only exists for a connection if the firewall has only seen traffic in one direction.
  - **ESTABLISHED**: The connection has been established and is a two-way communication.
  - **RELATED**: Special state that helps to establish relationships among different connections. E.g., FTP Control traffic and FTP Data traffic are related.
  - **INVALID** : This state is used for packets that do not follow the expected behavior of a connection.
- `iptables` can use `nf_conntrack` to build stateful firewall rules.



# Example: Set up a Stateful Firewall

```
// -A OUTPUT: Append to existing OUTPUT chain rules.  
// -p tcp: Apply on TCP protocol packets.  
// -m conntrack: Apply the rules from conntrack module.  
// --ctstate ESTABLISHED,RELATED: Look for traffic in ESTABLISHED or  
//           RELATED states.  
// -j ACCEPT: Let the selected packets through.  
  
$ sudo iptables -A OUTPUT -p tcp -m conntrack --ctstate  
    ESTABLISHED,RELATED -j ACCEPT
```

- To set up a firewall rule to only allow outgoing TCP packets if they belong to an established TCP connection.
- We only allow ssh and http connection and block all the outgoing TCP traffic if they are not part of an ongoing ssh or http connection.
- We will replace the earlier rule with this one based on the connection state.

# Application/Proxy Firewall and Web Proxy

- Inspects network traffic up to the application layer.
- Typical implementation of an application firewall is a proxy (application proxy)
- Web proxy: To control what browsers can access.
- To set up a web proxy in a network, we need to ensure that all the web traffic goes through the proxy server by:
  - Configuring each host computer to redirect all the web traffic to the proxy. (Browser's network settings or using iptables)
  - Place web proxies on a network bridge that connects internal and external networks.

# Application/Proxy Firewall and Web Proxy

- Proxy can also be used to evade egress filtering.
  - If a firewall conducts packet filtering based on destination address, we can evade this firewall by browsing the Internet using web proxy.
  - The destination address will be modified to the proxy server which defeats the packet filtering rules of the firewall.
- Anonymizing Proxy: One can also use proxies to hide the origin of a network request from servers. As the servers can only see the traffic after it passes through proxies, source IP will be the proxy's and actual origin is hidden.

# Evading Firewalls

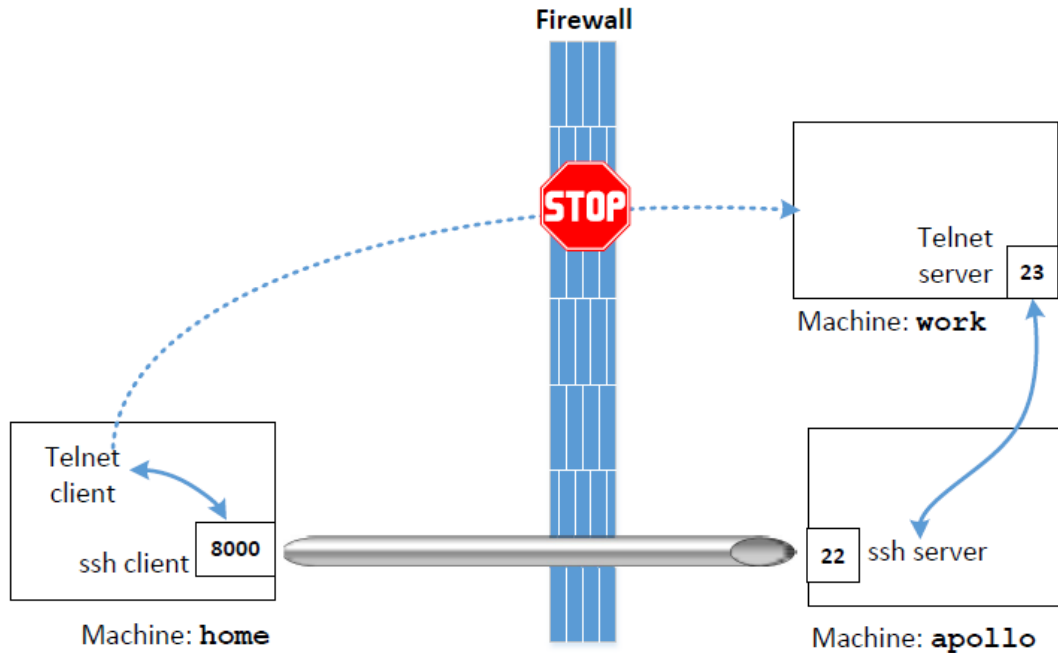
- SSH Tunneling
- Dynamic Port Forwarding
- Virtual Private Network

# SSH Tunneling to Evade Firewalls

## **Scenario :**

We are working in a company and need to telnet to a machine called “work”. Sometimes as we work from home, we need to telnet from machine “home” to “work”. However, the company’s firewall blocks all incoming traffic which makes telnet from “home” impossible. The company’s firewall does allow ssh traffic to reach its internal machine “apollo”, where we have an account. How can we use this machine to evade the firewall?

# SSH Tunneling to Evade Firewalls



- Establish a ssh tunnel between “home” and “apollo”.
- On the “home” end, the tunnel receives TCP packets from the telnet client.
- It forwards the TCP data to “apollo” end, from where the data is out in another TCP packet which is sent to machine “work”.
- The firewall can only see the traffic between “home” and “apollo” and not from “apollo” to “work”. Also ssh traffic is encrypted.

# SSH Tunneling to Evade Firewalls

```
// Establish the tunnel from Machine home to Machine apollo  
$ ssh -L 8000:work:23  apollo  
  
// Telnet to Machine work from Machine home  
$ telnet localhost 8000
```

- Establish an ssh tunnel from “home” to “apollo”. This tunnel will forward TCP data received on 8000 on “home” to port 23 on work.
- After establishing the tunnel, telnet to the 8000, and the telnet traffic will be forwarded host work via the ssh tunnel.

# SSH Tunneling to Evade Firewalls

**Scenario :** We are working in a company and working on a machine called “work”. We would like to visit Facebook, but the company has blocked it to prevent employees from getting distracted. We use an outside machine “home” to bypass such a firewall. How can we bypass it?

```
$ ssh -L 8000:www.facebook.com:80 home
```

- We establish an ssh tunnel from “work” to “home”.
- After establishing the tunnel, we can type “localhost:8000” in our browser.
- The tunnel will forward our HTTP requests to Facebook via home.
- The firewall can only see the ssh traffic between “work” and “home” and not the actual web traffic between “work” and “Facebook”.



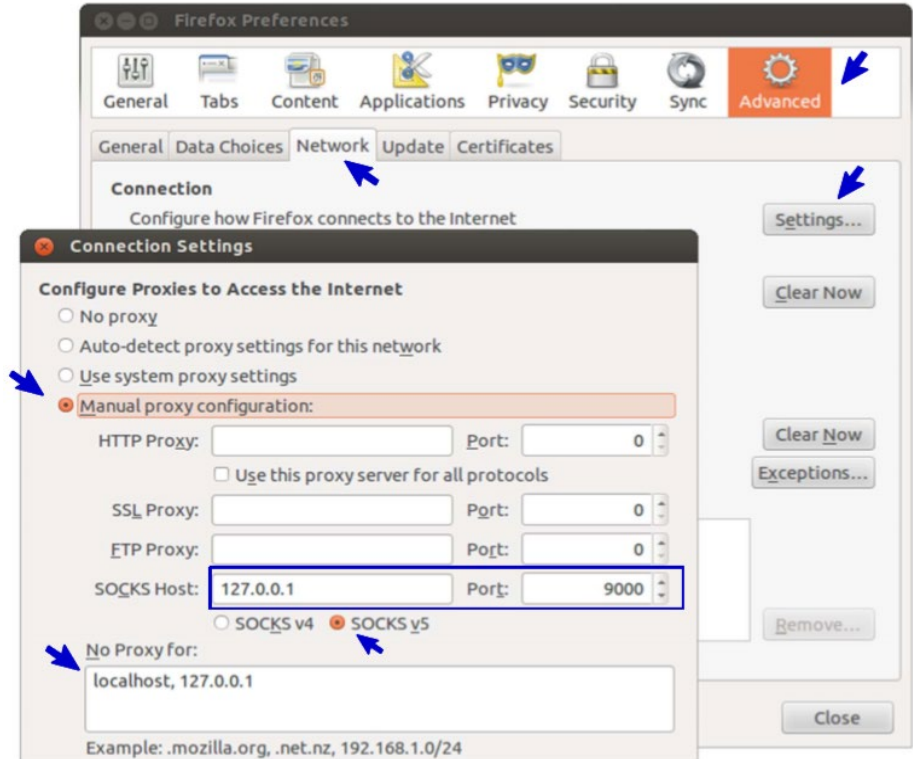
# Dynamic Port Forwarding

```
$ ssh -D 9000 -C home
```

- This command establishes an ssh tunnel between localhost (port 9000) and the machine “home”. Here we do not specify the destination for the port forwarding.
- So, we configure the browser in such a way that all the requests should go through localhost:9000, treating it as a proxy.
- Dynamic port forwarding that we set up using ssh is a **SOCKS proxy**.
- Once the browser is configured, we can type URL of any blocked site which will connect to ssh proxy at port 9000 on the localhost.
- ssh will send the TCP data over the tunnel to the machine “home” which will communicate with the blocked site.

# Dynamic Port Forwarding

The client software must have a native SOCKS support to use SOCKS proxies.



# Using VPN to Evade Firewall

Using VPN, one can create a tunnel between a computer inside the network and another one outside. IP packets can be sent using this tunnel. Since the tunnel traffic is encrypted, firewalls are not able to see what is inside this tunnel and cannot conduct filtering.

# Summary

- The concept of firewall
- Using iptables to configure a firewall
- Stateful firewalls and web proxy
- Bypassing firewalls