Network and application filtering; class 2

Baptiste HAMON, CISO

23/01/2019

**Internet** = Interconnection of Networks

### 1/ Reminder

OSI Layers

|  |  |
| --- | --- |
| Physical |  |
| Data Link |  |
| Network | IP |
| Transport | TCP, UDP |
| Session |  |
| Presentation |  |
| App | HTTP, FTP |

**Loopback address** = local host

IP protocols are “**unreliable**” : data corruption, arrival order of the packets, packet loss or destruction, duplication of packets…

Networks are made up of **hardwares** :

* Cables
* Network interface controller (NIC)
* Hub
* Switch
* Router

Why do we use port numbers?

* To communicate on different channels so information won’t collide.

Well known apps running as a server and listening for connections typically use the same ports :

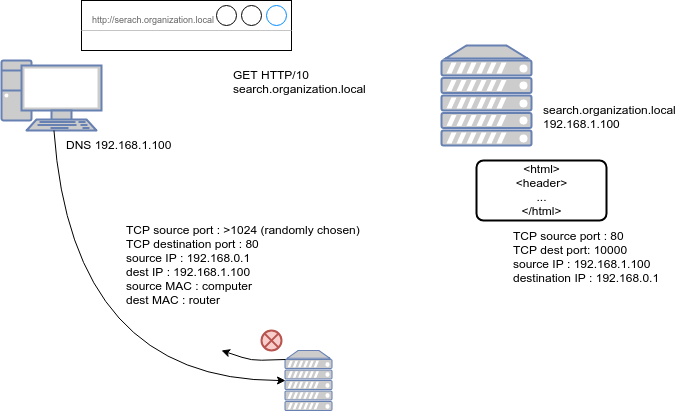
* HTTP : port 80
* HTTPS : port 443
* FTP : port 21

Protocols used by TCP (connected mode) :

* HTTP
* Integrity (ack, retransmission of segments)
* Flow control

Used by UDP (not connected mode) :

* Streaming (faster & less secure)
* Quick



VPN: system for creating a direct link between remote computers, they are on the same network

VPN IPSec : Authenticate and encrypt data : confidentiality + integrity

## Control the network

### Secure the internal network

* Network partitioning and filtering: user workstations, administrators desktops, printers, servers
* Firewall as first step after router: filter all the flows, are connected to each partitions

**Firewall**:

* Has an input bound tables and output bound tables to accept or deny accept
* Must cut the network
* Contains a set a rules allowing or prohibiting communications between machines
  + Read from top to bottom
  + Each packet is checked to the rule, if it doesn’t match then goes to next rule.
  + Last rule is any any drop. It is the cleanup rule: everything (what is not explicitly allowed) is forbidden
* To reject a packet:
  + Either : Explicitly return an error message to sender
  + Or : Do it implicitly
* Strengths of packet filtering
  + Reduction of servers exposure in one place (firewall)
  + Transparency
  + Fast flow
  + Available on multiple devices
* Issues of packet filtering
  + Any server can listen to any port (you can change the port) ⇒ your firewall will allow some ports, but if you put a SSH to listen on it, you can go through the firewall
  + Necessary to validate the application protocol, requires application filters

**Proxy** :

* Machine between local network and internet
* Allows to filter the connection from the client. ⇒ the administrator can download some .exe but the user can’t.
* Identification ⇒ who connects on the internet
* Validation of compliance to standard
* Filtering :
  + Whitelisting : allow specific websites =/= blacklisting
  + By content (key words…)

**Next-Gen Firewall :**

* Works more like proxy (works on the application layer)
  + Identification with IPS
  + Policy (allows / forbids some websites)
  + Signature system
* IPS (Intrusion prevention sys)
  + Analyze the signature of the files
  + Blocks the connection (=/= IDS which doesn’t)

**Reverse proxy http** :

* Filters the connection from the outside
* Blocks the SQL injections (doesn’t recognize the packets)
* Function of authentication (verification of strong authentication before reaching the server)
* Function of compression and load balancer

**Web application firewall :**

* Same as reverse proxy to protect app or service
* Works from 5th to 7th layer
* Inspects the traffic content and blocks it if bad
* Intercepts SSL/TLS
* Handles authentication for the web server