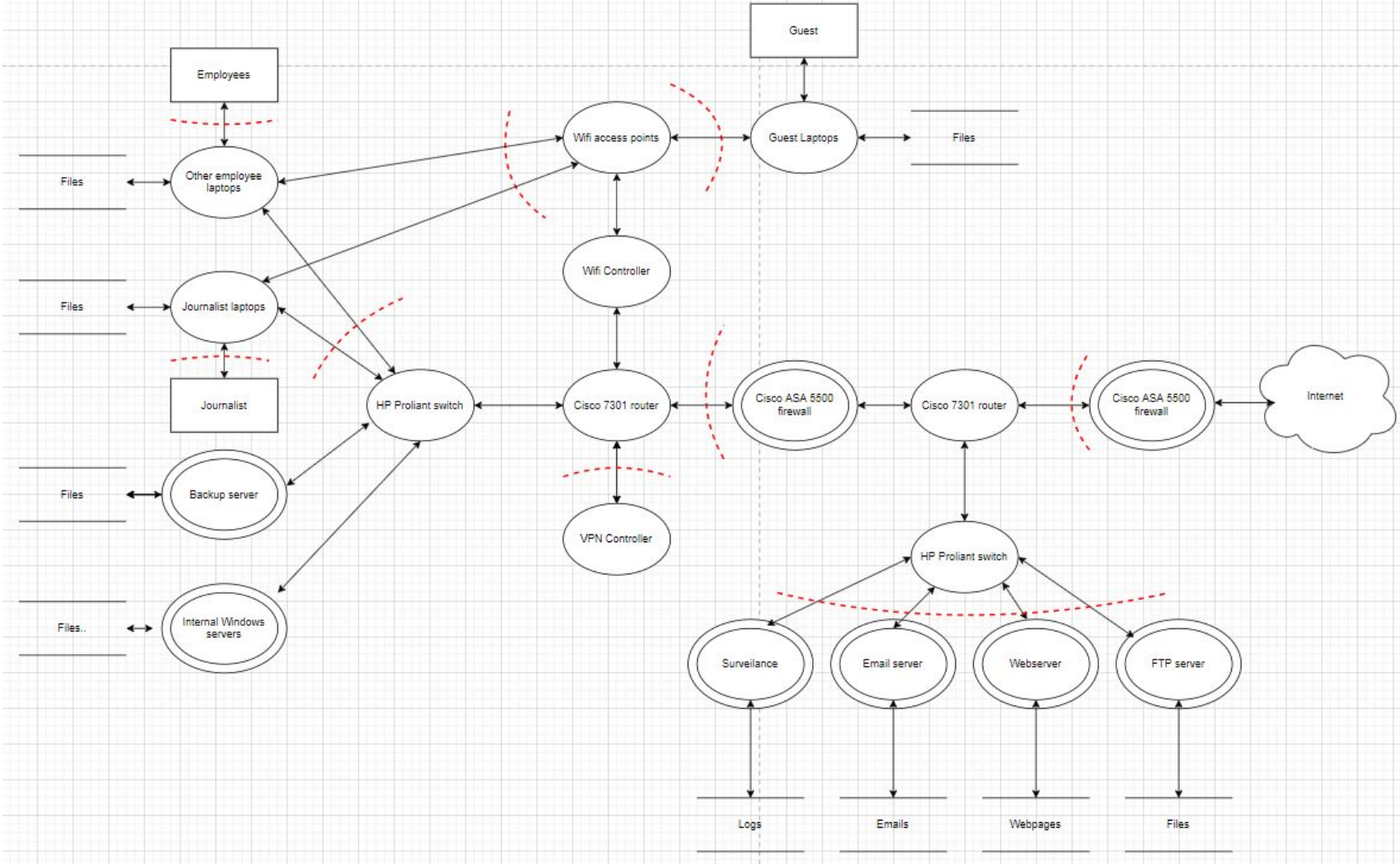
Group 17 Threat Model

Niklas Andersson, Jordy van Raalte, Josefin Andersson, Theo Le Magueresse

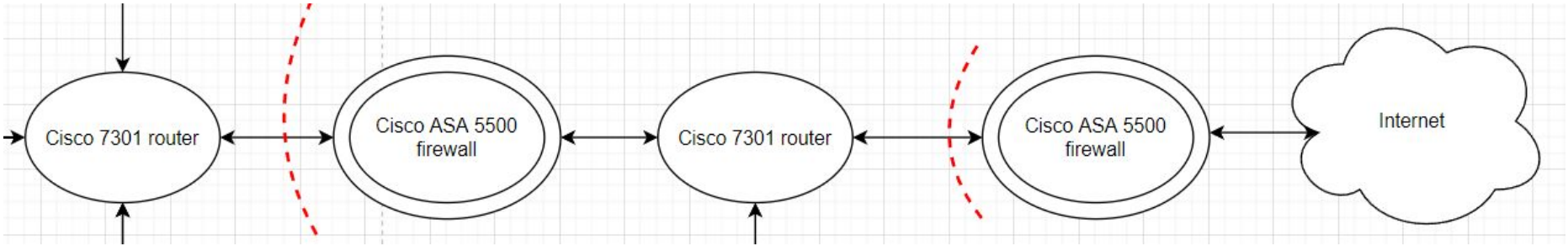

Guest
Employees
Wifi access points
Guest Laptops
Files
Files
Other employee laptops
Wifi Controller
Files
Journalist laptops
Journalist
HP Proliant switch
Cisco 7301 router
Cisco ASA 5500 firewall
Cisco 7301 router
Cisco ASA 5500 firewall
Internet
Files
Backup server
VPN Controller
HP Proliant switch
Files..
Internal Windows servers
Surveilance
Email server
Webserver
FTP server
Logs
Emails
Webpages
Files

Trust boundaries

Boundaries include:

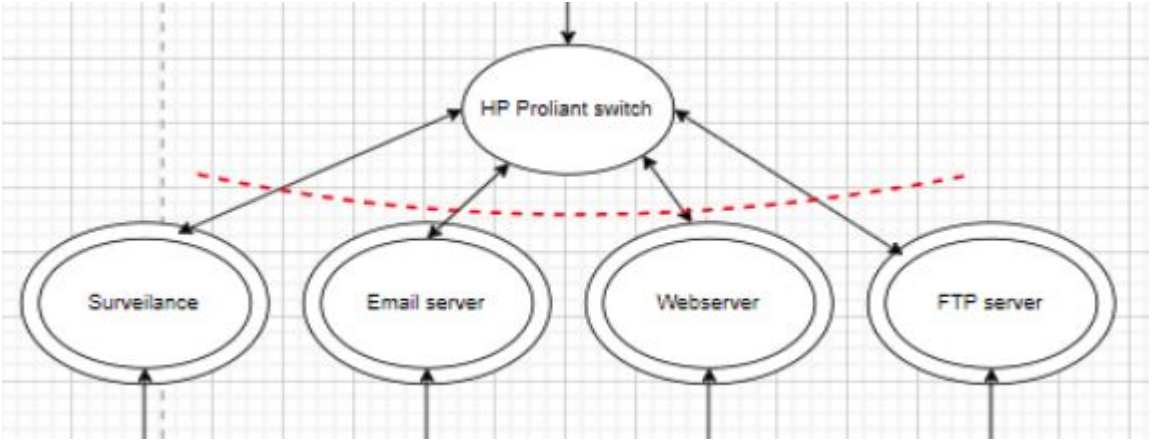
- Firewalls
- Employee laptops
- Wifi-access point
- Laptop access through HP proliant switch
- VPN controller

Firewalls



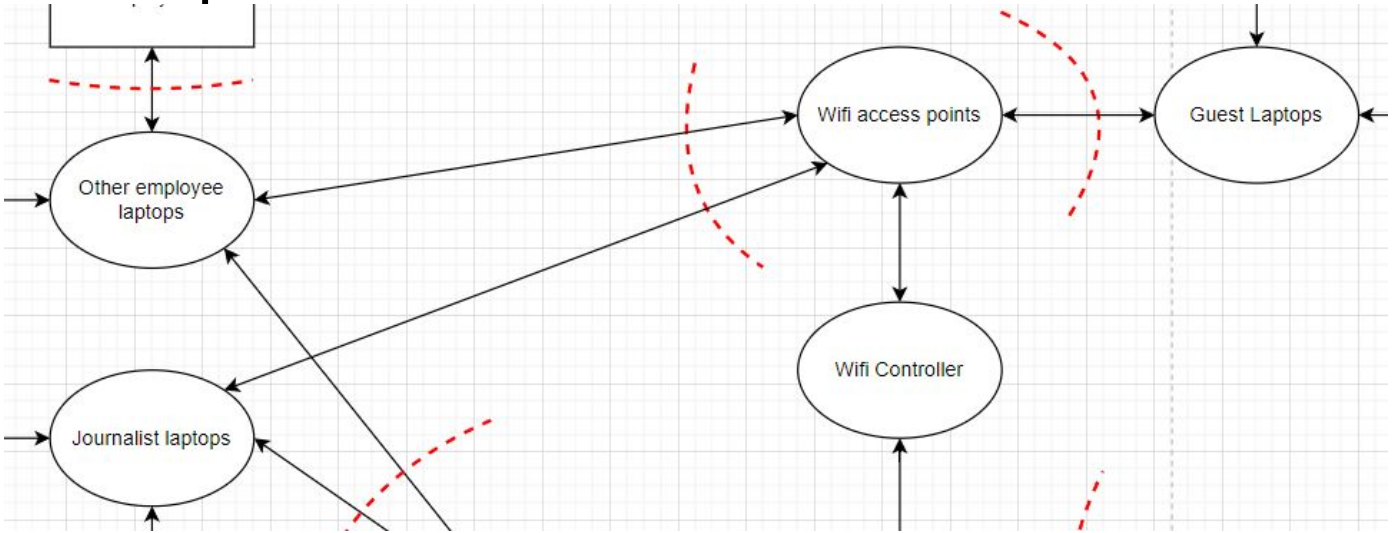
- The trust boundary after the first firewall, the one closest to the internet, is more lenient than the second. This is to accommodate the demands of easy access for tips etc.
- The second firewall is to the internal network and the trust boundary is a lot stricter in order to keep confidential information secure.

Servers



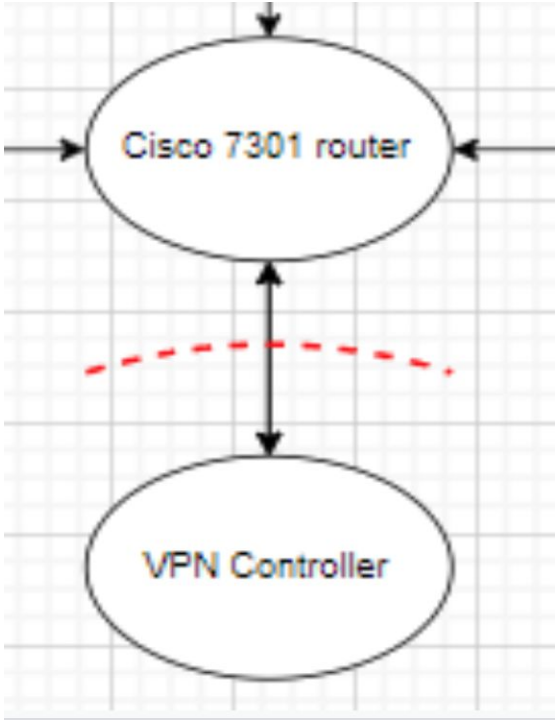
The servers contains a trust boundaries since the servers contains files that could be confidential and the integrity needs to be ensured.

WiFi Access point



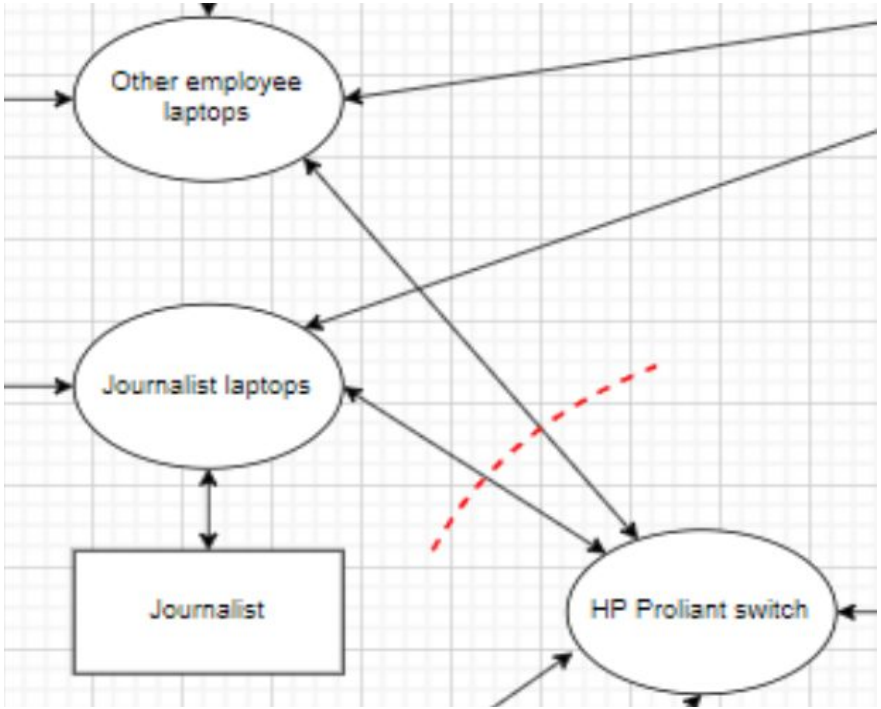
- The WiFi access point has a trust boundary to every user in order to not give access to the network to unauthorized users.
- Trust boundaries in a later stage restrict access for guests.

VPN controller



- The VPN controller has a trust boundary to has an extra controlled over the VPN network that has to be verified

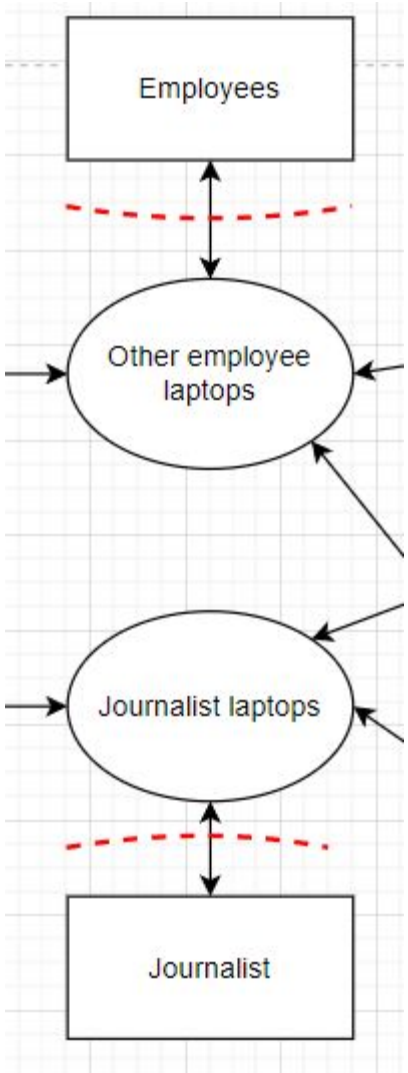
Laptop access through HP proliant switch



- Trust boundaries between the laptops and the switch is here to protect the network from infected laptops

Employee laptops

- Trust boundaries between the employees, both journalist and others exist.
- Trust in the authentication of user need to be established for the use of the laptops and the information contained.



Threats

Malware infection

Description

Multiple laptops from the employees, journalist and quests could be infected with malware. Also the servers can be infected with malware.

Consequences

Multiple- depending on the type of malware and its sophistication. Examples include: Denial of service, information disclosure, Tampering

Countermeasures

Already in place:

F-Secure Client Security anti malware software for the laptops

Recommended:

Anti malware software like F-secure client security anti malware software for servers.

Threats

Information disclosure

Description

An assailant might get access to valuable information assets within the Radio Sweden's network by exploiting vulnerabilities related to the entry points.

Consequences

Sensitive information might get exposed and further utilized to hurt the radio station and its employees.

Countermeasures

Access control

Device security policy