Astrid Strohmaier

Rovio – Satellite Office Setup

Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Bachelor's Thesis

01 Apr 2023

Abstract

Author:	Astrid Strohmaier, IT Service Specialist
Title:	Rovio – Satellite Office Setup
Number of Pages:	29 pages + 1 appendices
Date:	01 Apr 2023
Degree:	Bachelor of Engineering
Degree Programme:	Information Technology
Professional Major:	IoT and Networks
Supervisors:	Pekka Timonen, Senior Manager, IT Services (Head of IT) Tapio Wikström, Senior Lecturer Anne Pajala, Senior Lecturer

The objective of this thesis was to perform initial IT infrastructure installations and to create extensive process and installation documentation. It was carried out for Rovio Entertainment Corp. at their new studio locations.

Initially, a process for setting up new network, server and meeting room hardware did not exist; therefore, documentation was one of the main goals of this project. The project was carried out partially at Rovio's Espoo headquarters, where planning, equipment ordering, and initial configurations were implemented. Local installations in Izmir (Türkiye), Toronto (Canada), and Barcelona (Spain) were performed and documented.

The outcome of this project is that a comprehensive documentation was created. Guidelines for planning satellite office installations have been created, installation details were collected in setup documentation and multiple templates for easier organization were designed. Additionally, distribution lists and chat channels were set up for easier communication for all parties involved. Following the project, the satellite office installation process has been streamlined and can be carried out more efficiently.

Keywords: Firewall, Switch, Access Points, Domain Controller, Google Workspace

Contents

List of Abbreviations

Table of Contents

List of Abbreviations

AD:	Active Directory
AP:	Access Point
BGP:	Border Gateway Protocol
CLI:	Command Line Interface
DC:	Domain Controller
DHCP:	Dynamic Host Configuration Protocol
FW:	Firewall
HTTP:	Hypertext Transfer Protocol
iDRAC:	integrated Dell Remote Access Controller
IPsec:	IP Security
ISP:	Internet Service Provider
LDAP:	Lightweight Directory Access Protocol
NIC:	Network Interface Card
OS:	Operating System
PKI:	Public Key Infrastructure
PoE:	Power over Ethernet
PSK:	Pre-shared Key

RAID:	Redundant Array of Independent Disks
(R)STP:	(Rapid) Spanning Tree Protocol
SFP/SFP+:	Small FormFactor Pluggable
SW:	Switch
TCP:	Transmission Control Protocol
VGA:	Video Graphics Array
VLAN:	Virtual Local Area Network
VPN:	Virtual Private Network
WAN:	Wide Area Network

1 Introduction

Rovio Entertainment Corporation, a Finnish company creating mobile games, is expanding its business by creating new and acquiring existing game studios. These new studios are integrated into Rovio's IT network and server landscape. This thesis outlines the planning, implementation, and documentation phases for IT infrastructure setup at those locations.

The goal of this thesis project was to create a streamlined process for Rovio's satellite office installations and comprehensive documentation. The process includes documentation on planning and organizing, details on equipment to be purchased and installation guides for network, server, meeting room and other devices. While the Rovio-internal documentation contains detailed information on device naming and configurations, only brief overviews are given in this thesis paper and much of the details have been omitted for security purposes.

This paper contains 5 sections. Following the Introduction, Section 2 provides details and background to the project, followed by an overview of the devices used in Section 3. Section 4 lists parts of the device installations, followed by a Conclusion.

2 Project specification

Growth is a part of Rovio's strategy according to the official website (1). Opening new game studios or M&A (mergers & acquisitions) consequently require expanding the IT and network infrastructure. At the start of this project, Rovio had announced the opening of a new office in Toronto, Canada (2) and the acquisition of Ruby Games in Izmir, Türkiye (3). A comprehensive guide for performing the installation of networking equipment, servers, and meeting room equipment did not exist at that time; the existing documentation was focused on maintenance and troubleshooting tasks and did not include instructions for integrating new hardware into the infrastructure. Additionally, during the setup of

a satellite office in Montreal, Canada prior to the project commencement, problematic areas were identified, and it was decided to include documentation about the organizational factors of satellite office setup to mitigate or avoid similar problems.

The project work was carried out over multiple months during which the creation of another satellite office in Barcelona, Spain was announced (4). The documentation and guidelines created during the previous two installations provided constructive guidance for the Barcelona setup.

This section details the project specifications, including infrastructure planning, identification of possible complications, and lists the documentation that was created during the process.

2.1 Infrastructure planning

Rovio's new satellite locations may vary in office size, in the initial number of employees and location-specific requirements but were planned with possible future expansions in mind. A standard set of equipment was determined, which includes redundancy equipment in case of failures, and it also supports more than the initial number of employees at the new location. Note: for security reasons, sensitive information and configuration details have been included only in the Rovio-internal documentation and have been redacted from this thesis paper.

The table below lists the set of standard equipment for Rovio's satellite offices. For security reasons, remote access devices that are used for network troubleshooting from headquarters have been omitted from this paper.

Table 1. Standard set of equipment for Rovio satellite offices

Device	Manufacturer	Amount
Firewall (FW)	FortiGate	2
Switch (SW)	Cisco Meraki	2
Access Point (AP)	Cisco Meraki	3
Server (AD/DC)	Dell	1
Meeting room kit	Varied	Varied

Table 1 lists the standard devices Rovio uses in new offices, sorted by order of installation. Each new office is set up with 2 identical FortiGate firewalls for security and redundancy reasons. New offices are set up to support at least 60 Local Area Network (LAN) connections, so 2 Cisco Meraki switches are used. One of these switches supports Power over Ethernet (PoE), which is required for the wireless access points. As second switch, the same model but without PoE is used. By default, 3 Cisco Meraki access points to provide Wi-Fi access are prearranged per office; this number is either increased or reduced depending on the size and layout of each studio. A Dell server with a Windows Server operating system is installed and integrated into the existing Active Directory domain forest, if needed. The server may be omitted if it is feasible to use another DC from a close location. Meeting room kits vary; the manufacturer is often chosen by availability and the amount depends on the number of meeting rooms. Meeting room kits must support Google Meet, as this is Rovio's main meeting service. Except for meeting room kits, all the devices listed in table 1 are ordered to Rovio's headquarters in Espoo, Finland, where initial setup is performed before shipping them to the satellite office.

2.2 Problem areas

Throughout all satellite office preparations and installations, multiple problems were experienced. To mitigate or avoid similar problems in the future, recommendations on handling these were included in the satellite office documentation. Problems experienced include

- availability and delivery delays when ordering devices
- shipping delays when sending configured devices from headquarters to satellite offices
- satellite office renovation delays
- internet installation delays
- electrical installation delays
- tight schedules
- scheduling changes on short notice
- tombstone time

The list above shows that the problems mainly affect device availability and delays in equipment shipping and satellite office overall infrastructure installations. This sub-section outlines recommendations for handling these issues.

The availability of network and server equipment can vary, and it often takes multiple months until the devices are delivered. As solution, a standard set of equipment as detailed in section 2.1, except for a meeting room kit, is ordered to the Espoo headquarters as soon as one set of equipment has been sent to a new satellite office location. By following this recommendation, a set of equipment is always available for new satellite offices independently of current device availability.

The remaining items from the list above can be handled by improved communication and documentation, and by postponing local installations to a later date, since renovation schedules change. Communication has been improved by creating an email list including all IT-personnel involved in satellite office installations and by creating multiple channels in Rovio’s messaging app.

As renovations and building facility installations are usually delayed, pre-requisites for installation and delivery statuses were established prior to arranging travel dates for the IT team.

2.3 Satellite office setup documentation

The objective of this project was to create comprehensive documentation detailing not only the specific configuration of the network, server, and additional devices, but also to provide guidelines for infrastructure planning and organization of new satellite office installations. This sub-section gives a short overview of pre-existing documentation and lists the documents that were created for Rovio during this project.

Initial documentation was comprised of FortiGate firewall troubleshooting and maintenance guides, IP addressing information, lists of Active Directory (AD) groups and network documentation for some of Rovio's offices. Parts of the existing documentation were used as template for the new guidelines.

A master document was created that lists general information on the whole satellite office installation process and serves as guiding structure. The master document contains the following information:

- Details on communication, i.e., the mailing list and messaging groups used for discussing satellite office installations. A link to the template for a device/connection order tracking document is part of this section.
- A list of the standard setup, as discussed in section 2.1 (excluding meeting room devices).
- Explanations for device naming conventions for each location. For security purposes this thesis only mentions a part of each device name.
- Explanations for and a link to the existing document containing IP address reservations. IP addressing information has been omitted from this thesis paper.
- Physical setup and the order of device installation in the rack cabinet.
- Labelling, mounting, and cabling of devices.

- A link to the template for the network plan per satellite office.
- Links to the device configuration guides, including firewalls, switches, APs, AD/DC, and meeting rooms. These documents are ordered chronologically by installation sequence; explanations of what parts are done in the Espoo headquarters and in the satellite office are included.

An important document for planning a satellite network installation is the network plan for each satellite office. There, device models, and serial numbers are collected; device naming, and VLANs are planned and information regarding IP addressing is listed. Once an ISP has been found for the new office, their information is included in this document as well. Finally, a network diagram is drawn, showing the connections between the network devices, as shown in figure 1 below.

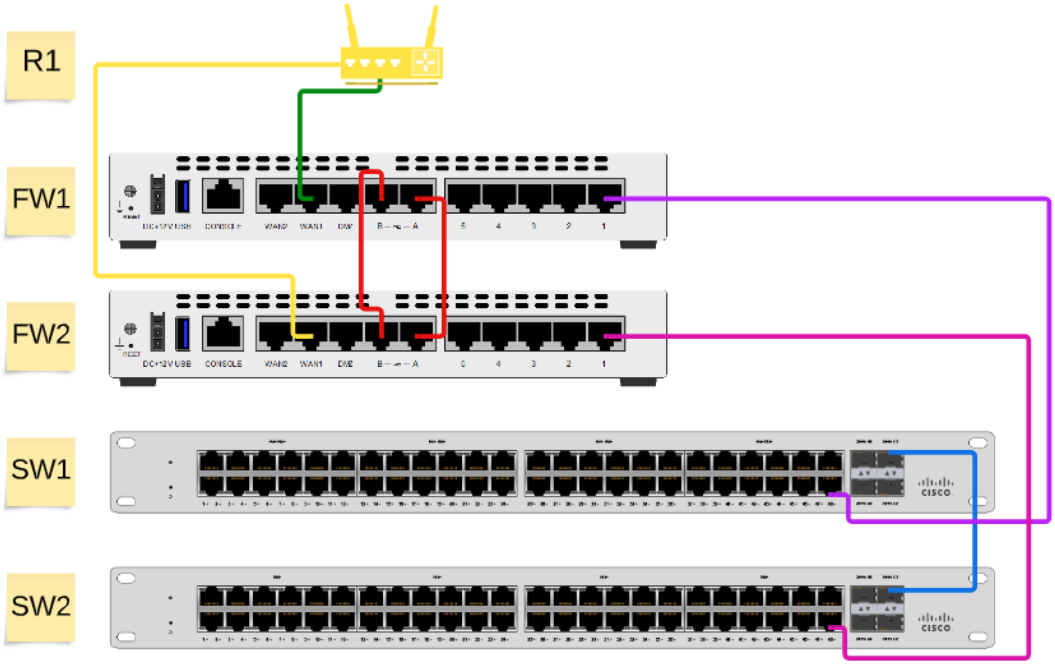

Figure 1. Network diagram template showing ISP router, firewalls 1 & 2 and switch 1 & 2.

The image above shows connections between the following devices:

- R1 is connected to FW1 on its WAN1 port
- R1 is connected to FW2 on its WAN1 port for redundancy
- SW1 port 48 is connected to FW1 port 1
- SW2 port 48 is connected to FW2 port 1 for redundancy
- SW1 port 51 is connected to SW2 port 51

In this example, devices are connected via Ethernet ports except SW1 and SW2, which are connected via SFP.

Details to the configuration guides for firewalls, switches, APs, AD/DC, and meeting room kits are discussed in later sections of this document.

3 Device overview

This section provides some background information on the devices used in satellite office installations and is based on the list of standard equipment in section 2.1.

3.1 Firewalls

Firewalls are fundamental in networking as they perform vital tasks to secure network traffic. Noonan and Dubrawsky (5, chapter 1) list the following firewall duties:

> manage and control network traffic, authenticate access, act as an intermediary, protect resources, record and report on events.

Rovio is using network-based firewalls, meaning separate devices that are directly connected to the ISP’s modem. All traffic going in and out of a Rovio office flow through the firewalls to ensure that the internal infrastructure is protected from potential threat-actors. Rovio is using different models of FortiGate firewalls, depending on the location of the remote office, distance to headquarters and availability.

As Rovio is a global company and employees can work from home, remote access into the company network is an important factor. To achieve this, a Virtual Private Network (VPN) is configured via FortiGate, using IP Security (IPsec). According to Noonan and Dubrawsky (5, chapter 10), the

> VPN policy needs to require the use of preshared keys and extended authentication, with the use of certificates, one-time passwords, and a full Public Key Infrastructure (PKI) for the most secure of environments.

Additionally, the VPN configuration includes which resources can be accessed from within each configured remote access network. Once VPN has been configured, Border Gateway Protocol (BGP) is configured, which handles routing inside the Rovio network.

3.2 Switches and Access Points

Switches are needed to provide the connections between devices in the office. The small office/home office (SOHO) LAN-model presented by Odom (6, chapter 2) loosely applies to Rovio's satellite offices. These SOHOs typically occupy one floor or a part of one floor in an office building and thus switches are only needed on one floor. Rovio is using 2 switches for specific reasons: the first switch is typically a Cisco Meraki switch supporting PoE (Power over Ethernet), which means that its ports can "provide electrical power for devices that may need it" (7), in Rovio's case to wireless access points (APs). To provide redundancy and ports for further LAN and network devices, the same switch model without PoE is used as switch 2. As the only devices needing PoE are a small number of APs, switch 2 does not need to support PoE.

Switch ports are configured by the function of the connected device; for separating network traffic, they are placed in different Virtual Local Area Networks (VLAN). By assigning different VLANs to dedicated ports, the local network can be split into various parts, which benefits security, problem solving and flexibility, among others as stated by Odom (6, chapter 8). As multiple switches and firewalls are used, uplink ports and ports to APs are set to trunk

port, whereas all other ports are set to access port. Trunk ports are required to add an extra header with the VLAN information when data travels between network devices (6, chapter 8).

Finally, to provide further redundancy, another protocol is required: Spanning Tree Protocol (STP), as “Using redundant links in a LAN design allows the LAN to keep working even when some links fail or even when some entire switches fail” as detailed by Odom (6, chapter 9). Rapid Spanning Tree Protocol (RSTP) provides redundancy and “RSTP prevents loops by placing each switch port in either a forwarding state or a blocking state” as detailed by Odom (6, chapter 9).

3.3 Server

Most satellite offices are equipped with one Dell server running a Windows Server operating system (OS), which is promoted to domain controller (DC). DCs “host the Active Directory database” according to Orin (8, chapter 4), which provides, amongst other functions, user authentication services via Active Directory (AD).

The DC is also set up as DNS (Domain Name System) server, to “translate host names to IP addresses and translate IP addresses to host names” according to Orin (8, chapter 5). Additionally, the DC is configured to provide IP addresses to LAN and Wi-Fi devices in the satellite office by functioning as DHCP (Dynamic Host Control Protocol) server.

3.4 Meeting room kits

Rovio uses Google Workspace as its main communication and collaboration tool; thus, meeting rooms are equipped with devices supporting the Google Meet technology (9). Depending on the meeting room size and function, as a minimum a small kit consisting of a camera, audio bar, Meet compute system and a remote control is installed. TVs are ordered directly to the satellite office and installed by building contractors while the meeting room kit is intended to be

installed by the visiting IT team. Apart from the initial device enrolment into the Google Workspace, the remaining configuration can be done remotely.

4 Device installations

This section deals with the physical setup and installation of firewalls, switches, APs, AD/DCs and meeting room kits. First, the physical setup of network equipment and servers in the rack cabinet is explained. Next an overview of the configuration of firewalls, switches & APs, and AD/DCs is given, followed by meeting room setup.

4.1 Preparations and physical setup in rack cabinet

Network and server equipment is ordered to the headquarters in the Espoo office for its initial configuration. Reasons for this include:

- When starting preparations for satellite office network and server installations, an address for the new office might not exist yet, so equipment orders cannot be placed to that location.
- The majority of IT is based in Rovio's headquarters.
- Network and server devices and their licenses are ordered from Finnish suppliers. Licenses are managed in Finland.
- The Espoo IT department is keeping IT equipment and peripherals in stock; thus, it is easier to obtain spare parts if needed.
- If devices turn out to be dead-on-arrival, it is generally easier to receive a replacement device to headquarters from an established supplier versus a new supplier in a different country. Also, language barriers could affect equipment ordering.

4.1.1 Rack installation

As part of creating a process for satellite office installations, a network lab has been set up in the Espoo office, consisting of a small rack cabinet and its peripherals, as well as a separate internet connection to protect the network in headquarters from misconfigurations. Figure 2 below shows the rack cabinet

with the current set of the Barcelona equipment before shipping to its destination.

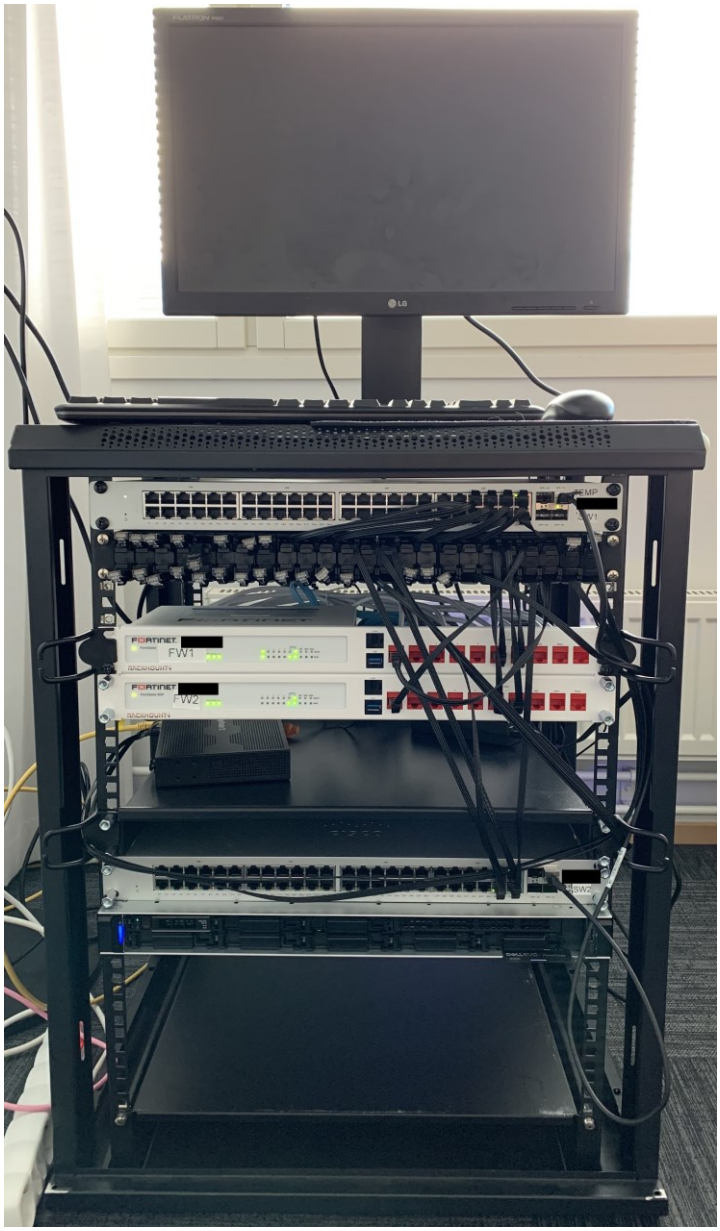

Figure 2. Rack cabinet with network devices and peripherals

The figure above shows a small rack cabinet containing peripherals (monitor with Video Graphics Array (VGA) port, keyboard, and mouse to connect to the server), a cabling system, cable organizers and a router for a separate internet connection. In this picture, the devices for the configuration of the Barcelona

office are mounted in the following order: SW1, Patchbox (cabling system), FW1, FW2, SW2, DC.

As comparison to the previous image, figure 3 below shows the rack cabinet of the Izmir office.

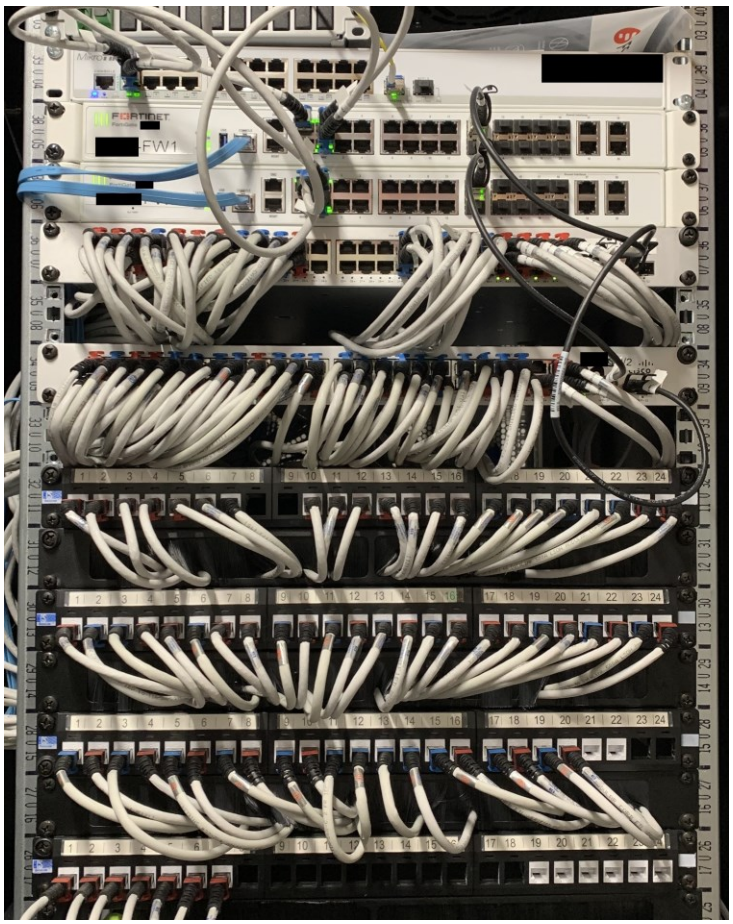

Figure 3. Rack cabinet of Izmir office

The image above shows the finished rack cabinet in Izmir. The devices are mounted as follows (from the top of the rack): ISP router, FW1, FW2, SW1, SW1, patch panels. The server is installed near the bottom of the rack and is not visible in this image.

Depending on office size and requirements, Rovio uses either Branch or Campus-level firewalls from FortiGate, as shown in Models and Specifications

on the Fortinet website (10). As branch firewalls are generally shorter than the rack cabinet width and they have their ports on the back side, they are encased into a rack mount kit. Figures 4 and 5 show Rovio's Toronto firewalls that are encased in a rack mount kit both from the front and from the back.

Figure 4. Toronto FortiGate rack mount kits, front side

As visible on the left in figure 4 above, the firewalls are inserted into their rack mounts with the LEDs to the front side. The ports, visible on the right side of the picture, are from the rack mounts.

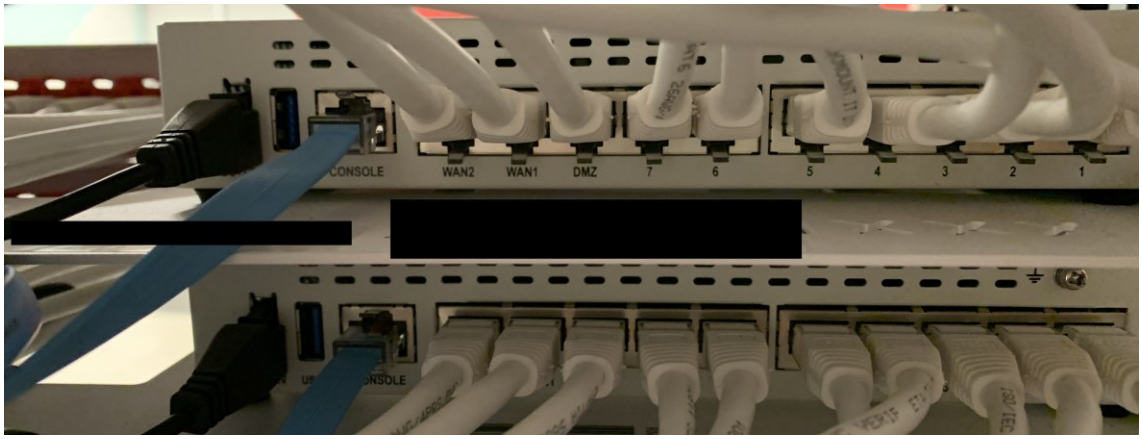

Figure 5. Toronto FortiGate rack mount kits, back side

Figure 5 shows the back side of the same firewalls as in figure 2. The ports are connected via short Ethernet cables to the back side of the rack mounts.

4.1.2 Cabling

Once the devices have been installed in the rack cabinet, they need to be cabled properly. The following table provides a quick overview of standard cabling.

Table 2. Cable connections between network devices and server

Device 1	Device 2
FW1, Wide Area Network (WAN) port	ISP router
FW2, WAN port	ISP router
FW1	SW1
FW2	SW2
FW1, High Availability (HA) port 1	FW2, HA port 1
FW1, HA port 2	FW2, HA port 2
SW1	SW2
SW1	APs
SW1	DC NIC1
SW2	DC NIC2
SW2	DC iDRAC
SW2	Door access control, if required
SW1	LAN devices
SW2	LAN devices

For redundancy purposes, both firewalls are connected to the ISP router. Also, each firewall is connected to a switch and both switches are connected to each other. To facilitate failover protection, the firewalls are connected to each other via 2 HA ports. With this configuration, Fortinet (11) assures that

> a cluster can provide FortiGate services even when one of the devices in the cluster encounters a problem that would result in the complete loss of connectivity for a stand-alone FortiGate unit.

As SW1 is generally the switch providing PoE, the APs are connected to ports on this switch. The servers usually have 3 Ethernet ports: 2 Network Interface Card (NIC) ports for internet access and an integrated Dell Remote Access Controller (iDRAC) port for remote administration. NIC1 of the AD/DC is connected to SW1, whereas NIC2 of the server is connected to SW2 for failover purposes. As the iDRAC port does not need PoE, it is connected to SW2.

LAN devices, such as meeting room devices and computers can be connected to either switch. PoE is turned off on SW1 ports where not required and all unused ports are disabled on both switches for security reasons.

4.2 Firewall installation

Since the firewalls are the only devices that are allowed to connect to the internet directly, they are configured first. After entering the license information on the Fortinet website, FW1 is connected via Ethernet cable to the computer which is being used to perform the configuration. An initial setup page is accessed via web browser; the first step is to change the administrative password to a more secure one; also, each firewall receives an individual name. The firewall configurations can be done either via Graphical User Interface (GUI) or via Command Line Interface (CLI), this section will show both methods interchangeably. The CLI is accessed from within a web browser as well. Extensive and detailed documentation has been created for Rovio’s IT team as part of this project, however, for security reasons, the configurations are not discussed in detail in this thesis document, and some are omitted.

First, FW1 needs to be configured to receive internet access. This is done in the sub-menu Network/Interfaces by editing the Internet interface, as shown in figure 6 below.

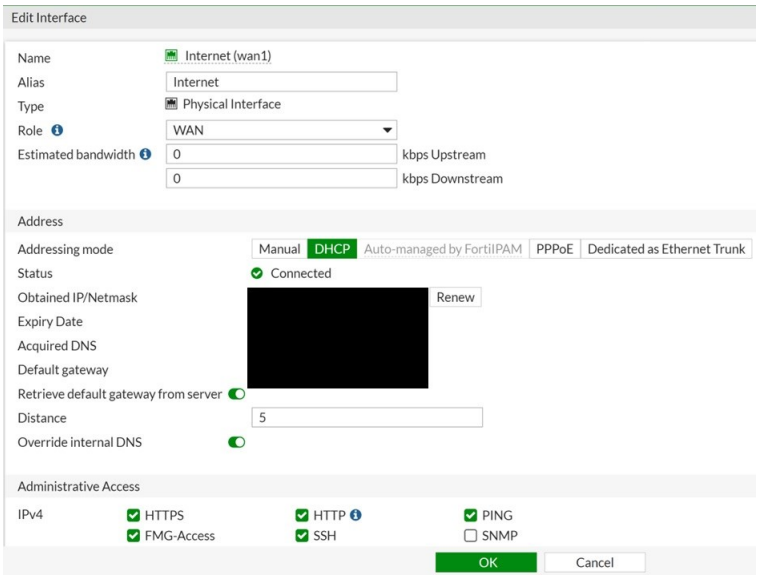

Figure 6. Editing the internet interface on FW1

Initially, the internet interface needs to be configured using DHCP, however, this is changed later during the configuration. The figure above shows a sample image of a firewall configuration via GUI. As it is a physical interface that is directly connected to the ISP router, its role is set as WAN.

Once internet access has been successfully set up, the firewall is upgraded to the latest firmware version in use. This can be done either via the web portal directly or by downloading a firmware image from the Fortinet website. To facilitate failover protection, the next step in the configuration is high availability (HA). First, FW1 is set to a higher priority in the HA configuration menu since it is the primary firewall. As next step, the management computer is connected to FW2, which is then configured with internet access, firmware upgrades and HA as well. FW2 is set to a lower priority. The following figure shows a successful HA configuration.

Figure 7. A successful HA configuration shown from FW1

Once the HA has been set up successfully, FW1 and FW2 are synchronized. The remaining firewall configurations are done only on FW1, as they are automatically synchronized to FW2. The synchronization status can be viewed in System/HA as shown in the figure above.

Next, interfaces need to be created to “allow traffic to flow between internal networks, and between the internet and internal networks” as detailed by Fortinet (12). Here, interfaces for management, LAN, internal Wi-Fi, server, and guest Wi-Fi are established. These interfaces are assigned a certain Virtual Local Area Network (VLAN) ID and IP address information, which are detailed in the satellite office setup documentation mentioned in section 2.3. At this point the DHCP server has not yet been configured, therefore FortiGate is set up to provide DHCP services to all interfaces initially. Objects corresponding to these interfaces can be created automatically or manually.

Next, policies need to be created to allow or deny traffic flow and afterwards administrative access is limited. To enable remote connections to Rovio’s network, a SSL (Secure Sockets Layer) VPN (Virtual Private Network) tunnel is established. To route internal network traffic successfully, internal Border Gateway Protocol (iBGP) is configured, following the example in the administration guide (13).

Next, services are configured, as shown in the following CLI listing.

```
config firewall service custom
     edit "HTTP"
          set category "Web Access"
          set tcp-portrange 80
     next
end
```

Listing 1. A CLI configuration showing a basic configuration of the Hypertext Transfer Protocol (HTTP) internet service.

The listing above shows a command line configuration of a service. The HTTP service is added to the category “Web Access” and set to Transfer Control Protocol (TCP) port 80. For security reasons further details have been omitted.

At this point of the installation, the firewall configuration pauses, as the AD/DC is needed for the next steps. During satellite office setup, however, switches and access points are configured next (see section 4.3), after which the domain controller (see section 4.4) is set up. Once the AD/DC has been configured successfully, the firewall configuration is resumed by setting up the newly installed server as Lightweight Directory Access Protocol (LDAP) server.

Interfaces are now modified, so that FortiGate does not provide DHCP services anymore, but a relay to the AD/DC. The following figure shows an image of an interface now using the AD/DC and its failover partner as DHCP relay instead of providing DHCP services.

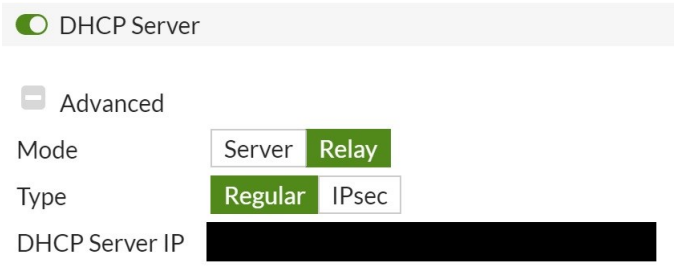

Figure 8. Interface being changed to DHCP Relay mode

Figure 8 shows an interface having DHCP Server enabled now in DHCP Relay mode instead of Server mode. Now the AD/DC is serving IP addresses and the firewall is simply pointing to it.

Depending on the local ISP, IT might receive the new satellite office IP information prior to the local installation. If this is the case, certain settings in the firewall can already be modified by changing the IP address information of the network lab router to the remote office's IP address, such as the internet interface's public IP. After this step, the devices need to be installed in the satellite office before continuing the configurations. In case there are any problems during shipping, it is crucial that the firewall configuration is downloaded and backed up before the devices are shipped to the satellite office.

Finally, once installed at the remote office, the last firewall configurations are done. VPN tunnels are added to Rovio's network monitoring, Simple Network Management Protocol (SNMP) is set up for fetching status information about the devices and firewall backups are configured. In some offices, door access control to the office space needs to be managed as well. To facilitate this, an interface separate from the internal LAN and Wi-Fi networks is created in a different VLAN. Depending on the requirements of the door access control device, policies are created to provide only the minimum required accesses, e.g. internet access is blocked if the device does not require it.

4.3 Switch and Access Point installation

Rovio is using Cisco Meraki switches, which can be configured via browser GUI or via mobile app. Like firewalls, first license information needs to be entered for the switches and APs used. Once done, a new network is created in the Meraki dashboard, as shown in figure 9.

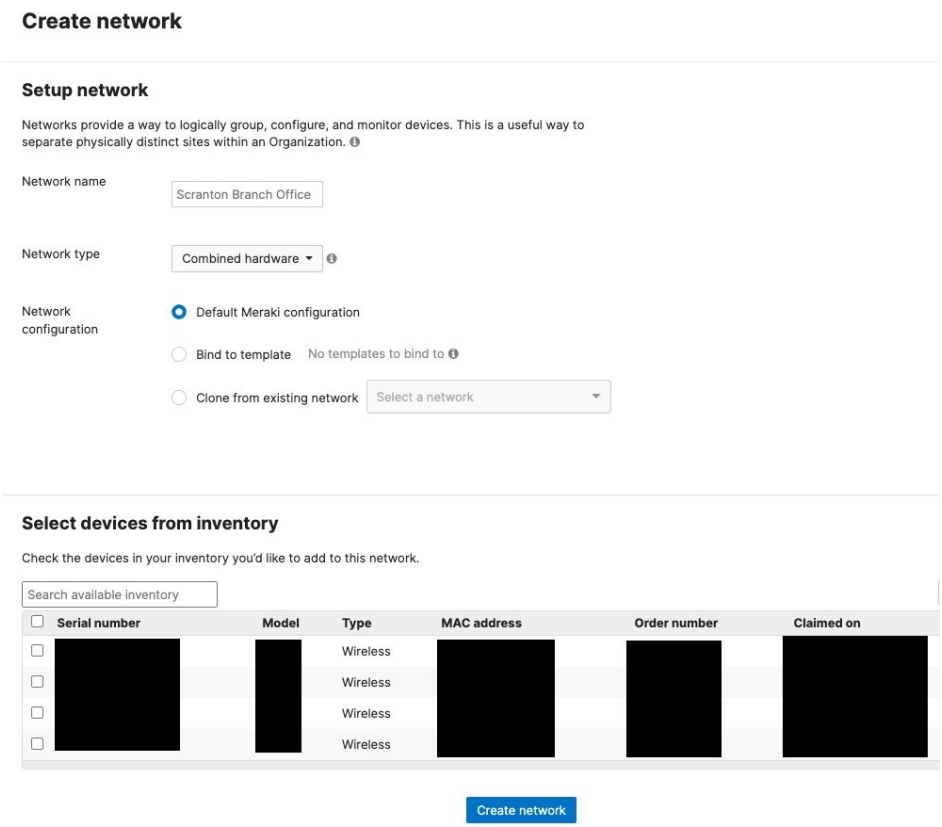

Figure 9. Creating a new Meraki network

The figure above shows the creation of a new network in the Meraki portal where naming and devices are assigned. Devices can also be added at a later point of the configuration, if, for example, additional APs are needed.

Once the devices have been named, they are upgraded if newer firmware is available. Next, Rapid Spanning Tree Protocol (RSTP) is enabled - STP configuration is shown in figure 10 below.

Figure 10. Enabling RSTP in Cisco Meraki

The image above shows RSTP enabling for Barcelona's SW1. The first switch is generally set up as root. It is important to verify that STP is turned off in the firewall, as some firewall models support STP settings as well, which would disrupt the network traffic.

Next, switchports are configured corresponding to their cabling as listed in section 4.1.2, starting from the highest port number. The last 4 ports on Cisco Meraki switches are Small Form-factor Pluggable (SFP/SFP+); SW1 and SW2 are connected to each other via these ports. Some firewalls have SFP+ ports as well, in which case they are used for the connection between switch and firewall. If the firewall does not have an SFP+ port, an Ethernet connection is used instead.

The following ports are reserved for APs. Since the access points are powered via PoE, SW1 must be a model supporting PoE. In situations where a PoE model is not available on time, a non-PoE model is used initially in connection with PoE injectors. PoE injectors are devices that are installed between a non-PoE switch and an AP. This solution has been used temporarily for the setup of Barcelona's switches, since the proper PoE switch was not available on time. The image below shows 2 different PoE injector devices.

Figure 11. 2 PoE injectors

Figure 11 above shows 2 PoE injectors from different manufacturers. Both have 2 Ethernet ports: PoE/DATA or PoE is connected to the AP while DATA/LAN is connected to SW1. The image below shows PoE adapters mounted in Barcelona's rack.

Figure 12. PoE adapters mounted in rack cabinet above switch.

The image above shows a side view of Barcelona's rack cabinet. As temporary solution until the proper switch can be delivered, all four APs in the office are powered via PoE injectors that are inserted between the switch and each AP. The PoE injectors are mounted in a rack shelf above the temporary SW1.

Next, a port for the server's NIC1 is configured on this switch. The following ports are either configured as access ports for LAN devices or disabled if they are not used. PoE is disabled for all non-AP ports. Figure 12 shows an overview of ports on a SW1.

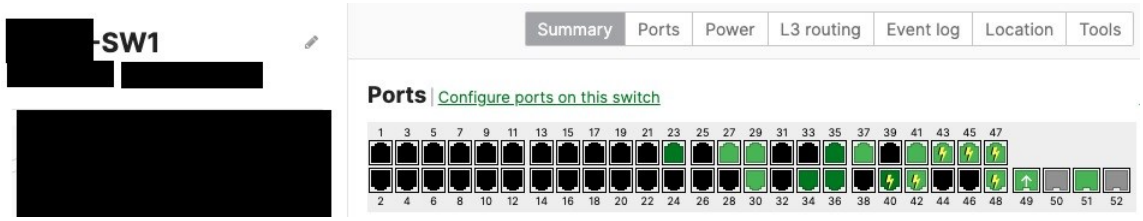

Figure 13. Ports on a SW1

The figure above shows 4 SFP+ ports (ports 49 – 52) and 48 Ethernet ports (ports 1 – 48). The lightning symbol identifies ports that are PoE-enabled.

SW2 is configured in a similar way, starting with SFP+ ports as connection to the other switch and to FW2, if supported. SW2 is connected to the server's NIC2, as well as to the server's iDRAC-interface. If door access control is required, the device is connected to SW2. The remaining ports are either configured as access ports or disabled if unused.

Finally, wireless access is configured to the access points. All satellite offices are provided with an internal Wi-Fi allowing access to Rovio's network resources, as well as a Guest Wi-Fi, which provides internet access for guests and non-Rovio supplied devices.

4.4 Server installation

An Active Directory domain controller providing DHCP services is installed in most satellite offices. This section gives an overview of the server's configuration. The image below shows Izmir's server mounted in its rack.

Figure 14. AD/DC in Izmir, view from backside.

Figure 14 above shows the backside of Izmir's server. Visible on the left are the 3 Ethernet connections: NIC1, NIC2, and iDRAC; their cabling was discussed in section 4.1.2. On the right side, 2 power cables are connected.

The server setup starts with booting into the Lifecycle Controller menu. There, iDRAC settings are configured first: iDRAC-name and IP-addressing information for the iDRAC-connection. As next step, NIC1 is configured with DHCP as address source, afterwards firmware updates are installed. After configuring Redundant Array of Independent Disks (RAID), the Windows Server OS is installed with Desktop Experience (i.e., providing a GUI in addition to a CLI). For redundancy and improved performance, NIC1 and NIC2 are grouped together in a NIC team via Windows Server Manager. Following this, the NIC team is configured with static IP addressing, after which the server OS is updated, security software is installed and other basic settings, such as naming the server are entered.

The next steps depend on the progress of the satellite office renovations and the estimated local installation timeframe: if it is likely that the estimated local installation will occur within the tombstone time, the server can already be configured in the headquarters. The tombstone time is important, as domain controllers replicate between each other. Should no replication occur within the tombstone time, objects in the domain are deleted according to Microsoft Learn (14 and 15). This would then need manual repairing of the Active Directory infrastructure and should be avoided. If the local installation is likely to happen

at a later date, the following setup is either delayed until shortly before shipping the devices to the new office or until the on-site installation.

First, the necessary server roles are added to the new server via Server Manager: Active Directory Domain Services, DHCP Server and DNS Server. Next, the server is promoted to domain controller. From another DC within the domain, a site is created in Active Directory Sites and Services; and once the new DC is visible there, the relevant subnets are added.

The new DC is then configured as DHCP server to provide IP addressing to devices in the network. The following image shows the configuration of an IP address range.

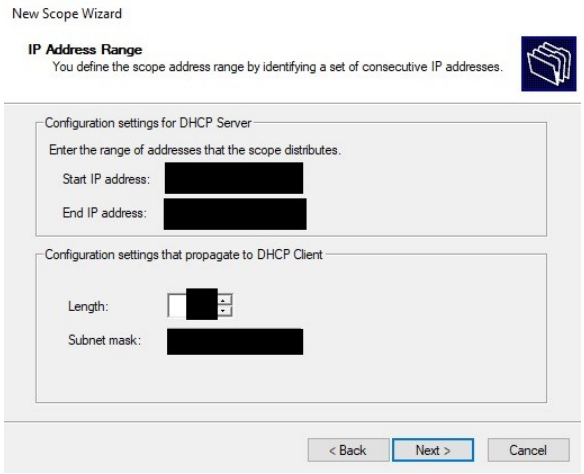

Figure 15. Adding IP address range to DHCP server

For each FortiGate interface that requires a DHCP server, the scopes are created as shown in figure 15. Once this has been completed, a failover relationship to provide redundancy and load balancing with one of the headquarters' servers is created. At this point, the DHCP service for those interfaces are changed in the firewalls to DHCP relay, as discussed in chapter 4.2. Finally, on any DC in the forest a service account is created, which will be used for the connection to a LDAP server in the firewall.

4.5 Meeting room installation

Due to renovation scheduling or delays, not all satellite offices are ready to receive meeting room equipment while IT personnel is visiting. In these cases, local personnel receive instructions on how to mount the equipment and assistance with enrolling the devices into the Google Workspace infrastructure. This section briefly discusses Google Meet setup.

Once the Google Meet devices have been mounted in the meeting room, they will need to be enrolled into the Google Workspace infrastructure. After the Meet compute system completes the device enrolment, the device checks its peripherals, such as camera, audio bar and display. Once completed, meetings can be booked locally, however, a calendar resource is not connected yet. The following two images show the installed meeting kit in one of Toronto's meeting rooms; Google Meet kits from Lenovo have been used in that office.

Figure 16. Meeting room in Toronto, showing the camera, sound bar, and remote

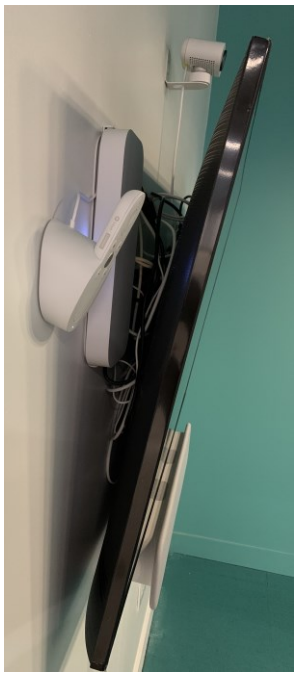

Figure 17. Same meeting room from the side, showing the Meet device behind the TV

Figure 16 above shows a front view of a Toronto meeting room. On this image, the camera, sound bar and the Meet remote are visible. Figure 17 above shows the same setup, but from the side. The Meet device itself is mounted behind the TV.

The remaining configuration can be done remotely by IT personnel since it only requires access to the Google Admin console and no physical access to the Meet devices. Prior to adding meeting rooms at a new location, the building first needs to be added to resource management. Figure 18 below shows the following step of adding a resource.

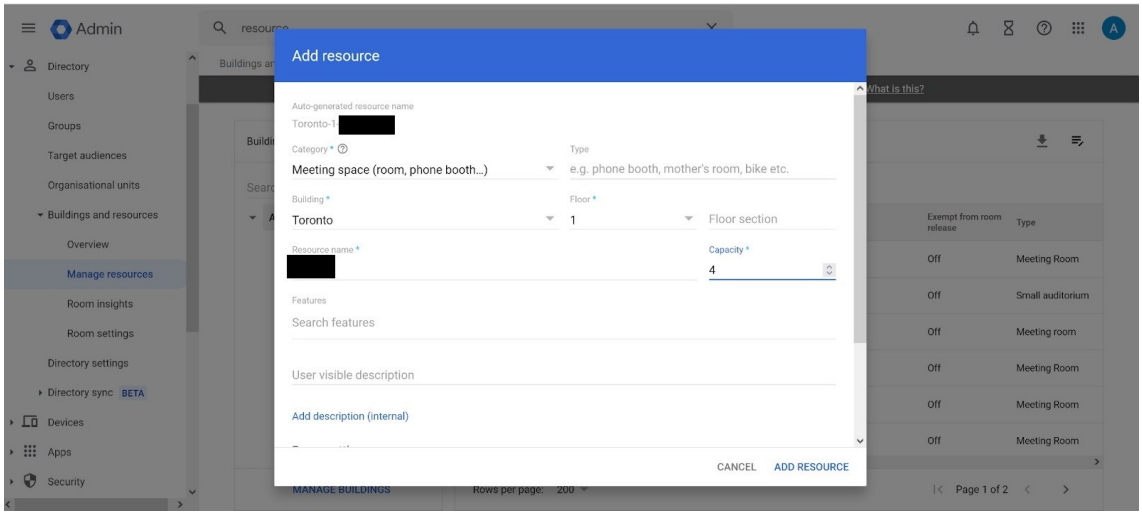

Figure 18. Adding resource to Google Workspace

The image above shows the sub-menu of adding a resource. As can be seen from the greyed-out text, the resource name is auto-generated, by combining the information from the building, floor and resource name information.

The next image shows Google Meet hardware in the Google Admin console.

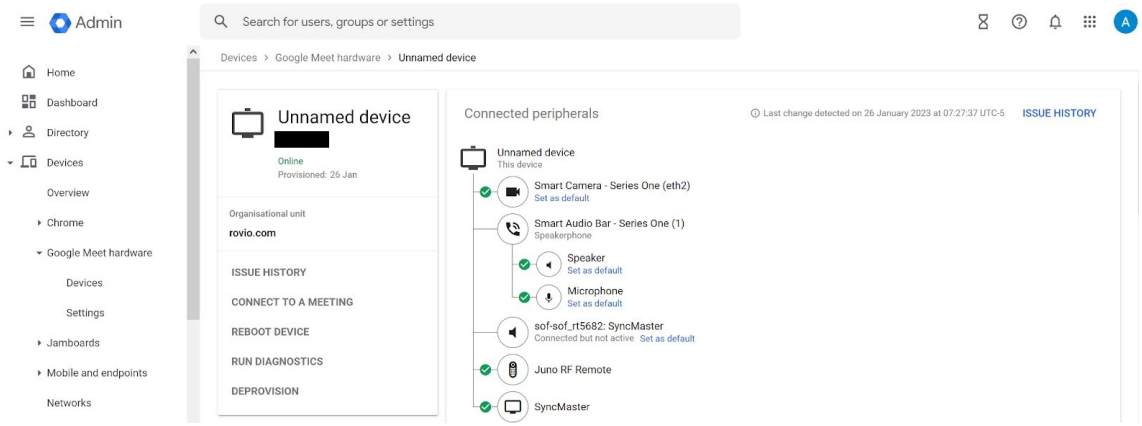

Figure 19. Google Meet hardware in Admin console

As shown in figure 19, all connected peripherals to a Google Meet device are visible in the Google Admin console. From here, a calendar resource is assigned to the device. After a reboot, the meeting room is now fully configured

with the basic settings and can be booked via Google Calendar. Additional settings, such as custom backgrounds can be configured in later steps as well.

5 Conclusion

As a result of this project, extensive documentation for satellite office setup has been created for currently ongoing and future installations. The documentation created consists of guidelines for planning and organizing satellite office installations, communication, details to equipment and comprehensive installation guides for firewalls, switches and access points, servers, meeting rooms, as well as devices used for administrative access. Additionally, Rovio's headquarters in Espoo, Finland were equipped with a network lab containing a small rack cabinet and peripherals.

The last installation executed during this project clearly showed an improvement in the process. While smaller details still needed to be added or modified, the on-site installation was carried out much more efficiently than the previous ones and was successfully completed on-site.

Satellite office installations that were implemented prior and during the project clearly showed that proper guidelines and documentation were needed. With a streamlined process, these installations can be planned and implemented more efficiently going forward. Additionally, communication and knowledge transfer have been improved, making information more easily accessible by all parties involved.

References

1 Our strategy [Online] Rovio Entertainment Corp. URL: https://investors.rovio.com/en/about-us/our-strategy. Accessed 9 March 2023.

2 Introducing Rovio Toronto! [Online] Rovio Entertainment Corp. URL: https://www.rovio.com/articles/introducing-rovio-toronto/. Accessed 2 October 2022.

3 Rovio Entertainment acquires hyper-casual game studio Ruby Games [Online] Rovio Entertainment Corp. URL: https://www.rovio.com/articles/rovio-entertainment-acquires-hyper-casual-game-studio-ruby-games/. Accessed 2 October 2022.

4 Introducing Rovio Barcelona [Online] Rovio Entertainment Corp. URL: https://www.rovio.com/articles/introducing-rovio-barcelona/. Accessed 24 November 2022.

5 Noonan, Wesley J. & Ido Dubrawsky. Firewall Fundamentals [e-book]. 2006. Cisco Press [cited 19 March 2023]. Available from: https://learning.oreilly.com/library/view/firewall-fundamentals/1587052210/.

6 Odom, Wendell. CCNA 200-301 Official Cert Guide Library [e-book]. 2019. Cisco Press [cited 19 March 2023]. Available from: https://learning.oreilly.com/library/view/ccna-200-301-official/9780136755562/.

7 Meraki Go - What is PoE (Power over Ethernet)? [Online] 2021 Cisco Systems, Inc. URL: https://documentation.meraki.com/Go/Meraki_Go_-_What_is_PoE_(Power_over_Ethernet). Accessed 13 March 2023.

8 Orin, Thomas. Windows Server 2019 Inside Out [e-book]. 2020. Microsoft Press. (2020). [cited 19 March 2023]. Available from: https://learning.oreilly.com/library/view/windows-server-2019/9780135492222/.

9 Google Meet [Online]. Google Workspace. URL: https://workspace.google.com/intl/en/products/meet/. Accessed 13 March 2023.

10 Next-Generation Firewall (NGFW) [Online]. 2023 Fortinet, Inc. URL: https://www.fortinet.com/products/next-generation-firewall. Accessed 13 March 2023.

11 Failover protection [Online]. Fortinet. URL: https://docs.fortinet.com/document/fortigate/6.4.12/administration-guide/489324/failover-protection. Accessed 13 March 2023.

12 Interfaces [Online]. Fortinet. URL: https://docs.fortinet.com/document/fortigate/6.4.12/administration-guide/154471/interfaces. Accessed 13 March 2023.

13 Basic BGP example [Online]. Fortinet. URL: https://docs.fortinet.com/document/fortigate/6.4.12/administration-guide/763341/basic-bgp-example. Accessed 13 March 2023.

14 Active Directory Replication Concepts [Online]. Microsoft. 10/08/2021. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/replication/active-directory-replication-concepts. Accessed 13 March 2023.

15 Information about lingering objects in a Windows Server Active Directory forest [Online]. Microsoft 02/23/2023. URL: https://learn.microsoft.com/en-US/troubleshoot/windows-server/identity/information-lingering-objects. Accessed 19 March 2023.

FortiGate CLI excerpt

```
show system admin
config system admin

show system interface
config system interface

show firewall address
config firewall address

show router prefix-list accept-from-izmir
show router prefix-list advertise-to-izmir
config router prefix-list

show router bgp
config router bgp

show firewall service custom
config firewall service custom

show user ldap
config user ldap

show user group
config user group
```