



Expertise
and insight
for the future

Joni Paavola

Company grade network at home

Metropolia University of Applied Sciences

Bachelor of Engineering

Internet Technologies

Bachelor's Thesis

10 October 2021

Abstract

Author: Joni Paavola
Title: Company grade network at home
Number of Pages: 37 pages
Date: 12 October 2021

Degree: Bachelor of Engineering
Degree Programme: Internet Technologies
Professional Major: Networking
Supervisors: Marko Uusitalo, Senior Lecturer

The goal for this engineer project was to create a company-like network at home. The reason for creating it was to introduce a home network with similar qualities than a company network regarding security, usability, and possibility to access files remotely.

The project was inspired by mid-sized company networks. After pondering the idea carefully, the planning started: how to get access to needed software and hardware, what kind of software and hardware is needed, and what is needed to take them into use. After getting the needed devices and programs, installation started. It took a while because the basic information gained at school was not enough but needed some work experience. Information from school worked as a base for learning more. It took hours of self-learning and practical work after assembling the server from components and installing Windows Server and Active Directory. Google was an important tool to find documentation and troubleshooting material.

Gradually, ideas were performed in practice. As the result, there was a secure network, that was easy to use remotely and to manage, as well as using it locally.

In conclusion this final year project took a lot of time and effort, However, the results were good and useful as working life experience. At home the results can be used to create a secure network environment for work and leisure.

Keywords: network, firewall, active directory

Tiivistelmä

Tekijä: Joni Paavola
Otsikko: Yritystason verkko kotona
Sivumäärä: 37 sivua
Aika: 12.10.2021

Tutkinto: Insinööri (AMK)
Tutkinto-ohjelma: Internet teknologiat
Ammatillinen pääaine: Verkko
Ohjaajat: Lehtori Marko Uusitalo

Insinööriyön tavoite oli toteuttaa yritystason verkko kotiin. Sen tarkoitus oli tuoda kotiverkolle samanlaisia elementtejä, kuin yritysverkossa on, eli esimerkiksi tietoturvaa, käytettävyyttä ja mahdollisuus yhdistää etänä siten, että tiedostoihin pääsee käsiksi.

Keskikokoisten yritysten verkot toimivat inspiraationa tätä projektia varten. Kun ajatusta oli pohdittu, suunnittelu alkoi. Tuli etsiä tietoa siitä, mistä ja millaiset laitteet ja ohjelmistot pitää hankkia. Kun hankinnat oli tehty, aloitettiin asennustyö. Koulussa opittu ei ollut riittävää, vaikka se toimikin pohjana projektille. Opinnot olivat kuitenkin tärkeitä pohjana sille, mitä projektin aikana tuli opittua hakemalla lisää tietoa, työelämässä ja kotona. Asennus alkoi kokoamalla palvelin osista, ja Windows-palvelinkäyttäjärjestelmän asentamisella. Active Directory-roolin asentamisen jälkeen alkoi hankalampi osuus, jossa tuli etsiä tietoa aktiivisesti ja tehdä työtä asia kerrallaan.

Uusia ideoita tuli matkan varrella ja niitä tuli hyödynnettyä aktiivisesti. Lopulta syntyi toivottu lopputulos, eli turvallinen verkko, jota oli helppo hyödyntää etätöihin ja vapaa-aikaan, sekä myös paikallisesti.

Insinööriyön aikana kertynyttä uutta tietoa ja kokemusta on voinut hyödyntää työelämässä, sekä kotona vapaa-ajalla.

Avainsanat: verkko, palomuuuri, Active Directory

Contents

List of Abbreviations

1	Introduction	1
2	Domain Controller	3
2.1	Basic configuration	4
2.2	Advancing in configuration	8
2.2.1	Certificate Authority	8
2.2.2	NPS	8
2.2.3	AAD Connect	8
3	Network	10
3.1	Firewall	10
3.1.1	Initial setup and introduction	11
3.1.2	Remote Access VPN	17
3.2	RED	23
3.3	Wireless Local Area Network (WLAN)	24
3.4	Switching	26
4	Workstations	29
5	Microsoft 365	31
5.1	Licensing	31
5.2	Intune and Endpoint Management	33
6	Conclusion	Virhe. Kirjanmerkkiä ei ole määritetty.
	References	36

List of Abbreviations

AAD	Azure Active Directory. A Microsoft cloud directory service, similar to on-premises Active Directory.
AD	Active Directory. A Microsoft directory service for example for users, groups, computers and configurations.
AP	Access Point.
DHCP	Dynamic Host Configuration Protocol. A protocol, which is used to distribute IP addresses, Gateway IP addresses and DNS server IP addresses to servers, workstations, mobile devices, printers etc.
DNS	Domain Name System.
GB	Gigabyte. A unit of size of data.
HDD	Hard Disk Drive. A non-volatile storage memory drive with spinning disks.
IP	Internet Protocol. A protocol which is used to communicate with and access other devices in network. A device needs an IP address in order to communicate with network devices.
IPS	Intrusion Prevention System.
LAN	Local Area Network. A network, used locally at office, home or public place.
NAP	Network Access Protection.
O365	Microsoft Office 365.
RAM	Random Access Memory. A volatile memory, keeps running operating system and applications until powered off.
RDP	Remote Desktop Protocol. A Microsoft protocol used to control workstation's or server's desktop remotely.

RED	Remote Ethernet Device. A networking device to provide branch offices with SD-WAN connection.
SSD	Solid-State Drive. Non-volatile flash storage memory drive.
SSID	Service Set Identifier. A name/identifier of WLAN network.
SSL	Secure Socket Layer. Used for encrypting connections, proving identity with certificates etc.
TB	Terabyte. A unit of size of data.
UPN	User Principal Name.
VoIP	Voice over IP. A protocol used to communicate with other people over Internet Protocol using voice.
VPN	Virtual Private Network. A network between remote locations.
WAN	Wide Area Network. For example, internet.
WLAN	Wireless Local Area Network. A wireless network, used locally at office, home or public place.

1 Introduction

The goal of this study was to create a company grade network with access, security, and usability. More detailed, to access file server, server management, firewall administrator interface and security cameras from internet and using Remote Desktop Protocol, RDP, to manage the server or workstations . The network needs to be secure, also the Wireless Local Area Network, WLAN. There also needs to be a site for Virtual Private Network, VPN to a remote network connection without a firewall. The remote network connection must be secure, so all the connections should go through the tunnel to be inspected by firewall at main location. See figure 1.

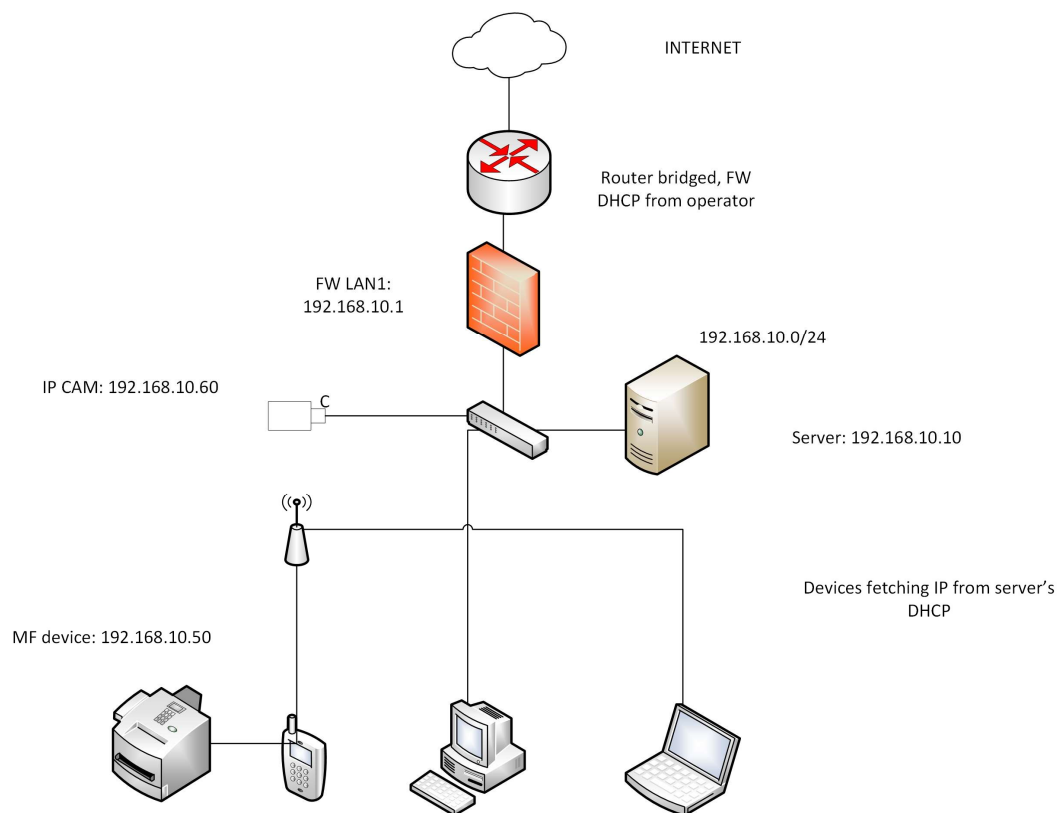


Figure 1. Network diagram.

To proceed, a firewall device and license, company grade WLAN Access Point, server computer with Windows Server, security cameras and workstations are needed.

Also, the remote site needs to have a Software Defined WAN connection to connect main location.

For primary WLAN, SSID that uses Active Directory credentials securely will be used for authentication.

For Guest SSID, using a Hotspot with different kind of authentication will be used. The Guest SSID should be isolated from primary network. It should also be used in a way that makes it more difficult for a hacker to crack into it to use bandwidth for criminal activities.

Workstations must have a workstation security; the best is yet to be decided. It has to be able to block all kinds of malware, not just basic viruses. Signature-based detection is not enough, and crypto malware must be detected and blocked, as well as the files need to be safe from illicit encryption.

The set should also have remote controlled alarm system that is triggered by motion or open doors, to check the security cameras remotely.

It should have a multifunction device that can send emails and Microsoft 365 with custom domain, email addresses, email security, encrypted emails, and Azure Active Directory sync from On-Premises Active Directory with needed attributes.

Minimum operating system for domain workstations is Windows 10 Professional to use them in the Active Directory Domain.

This is all done to make the network more secure, and easy to use also remotely. When buying a new computer, there is no need to set up user accounts and basic programs to it, because all is ready in the server. Also, basic Endpoint management and Intune setup are good to have for modern approach to push install applications and to have endpoint information at quick reach and to distribute applications that can be downloaded easily from Company portal.

2 Domain Controller

Domain Controller is a Windows based server, which is used, as the name says, to control a Windows Domain. Minimum services that are used with it, are for example Active Directory Domain Services and DNS. Often also DHCP service is within a domain, instead of a networking device such as a firewall, router etc. Active Directory is used to manage user accounts, computer accounts, user groups and Group Policies, for example. User accounts are often used domain wide to log in to the domain joined workstations, to access the services in domain such as file services, printer services and also organizations cloud services such as Azure Active Directory, and Azure Enterprise apps. [1]

Group Policy is used to distribute policies across domain. It has a wide variety of different policies, such as printer distribution, mapping network drives, push installing different applications and lots of security policies.

DNS is used for retrieving a name against an IP address. Domain joined workstations are asking the DNS server what the IP address for a name is. DNS server is often pointing to external DNS servers higher in hierarchy if some host is not found inside a domain. It will retrieve an IP address for a name, when for example a workstation is trying to reach URL like <https://www.google.com>.

The workstation requests an IP address from DNS server, which finds out it does not know it, asks it from another DNS server, which then replies with an IP address, and the server forwards it to the workstation (when forwarders are used, instead of directly distributing the DNS servers located on the internet).

DHCP is used to distribute IP addresses to the domain computers, which use a setting that does not specify a static IP address. A workstation cannot use network resources in local area network or internet without having a proper IP address, knowledge of DNS server and a gateway, if a host it tries to reach is located outside its own network. Without IP address, a workstation sends a request through its network interface for an IP address information. The request is called DHCP request. DHCP server replies a request with IP address information and the workstation is then configured with the needed IP information.

Active Directory user groups, for example security groups, are used to give certain properties or permissions to users, which are in groups. For example, file server permissions are often done with group permissions.

To make it clear and understandable for other administrators, a group is given such a name that tells what it is used for. If the file server has different folders for different teams in an organization, one for management, one for sales and one for warehouse, the user groups as well as the file folders could be called Management, Sales and Warehouse.

But often different teams have cross-folder permissions, just like Sales must have minimum Read permission to Warehouse folder. Then the clearest way to perform this is to create two security groups per folder: Warehouse_R, Warehouse_RW. Sales group would be added into Warehouse_R group, and the warehouse workers would belong into Warehouse_RW. This would be performed to every folder to enable R and RW groups. [2]

2.1 Basic configuration

Server operating system had to be chosen and it is Windows Server 2012 R2. Windows Server 2012 R2 was at the time the Windows Server operating system available for this project, and it had the needed functionality.

Domain services were installed, as well as DNS (Dynamic Name Server) and DHCP (Dynamic Host Configuration Protocol) server services, as well as File and Storage services. The services, respectively, are to ensure that networking works as it should. First of all that the names can be translated to IP addresses, and then also the devices in the network will get automatic network configuration.

Names must be translated to IP addresses to solve for example in which IP address the domain controller and other devices in the network are.

Without IP address there is no communication. IP can be static or automatic. Automatic IP configuration is given by the DHCP server, because mainly the devices are not given static IP and especially in big network it would cause lots of extra working hours.

The workstation, mobile device, or any device in network, will send a query to network asking if there is a DHCP server willing to give IP address configuration, including the private IP for the device itself, the netmask and the default gateway information, as well as the means for name resolving, the DNS server IP address. DHCP then answers, and they continue the discussion until the device has set their IP address configuration. [3] See figure 2.

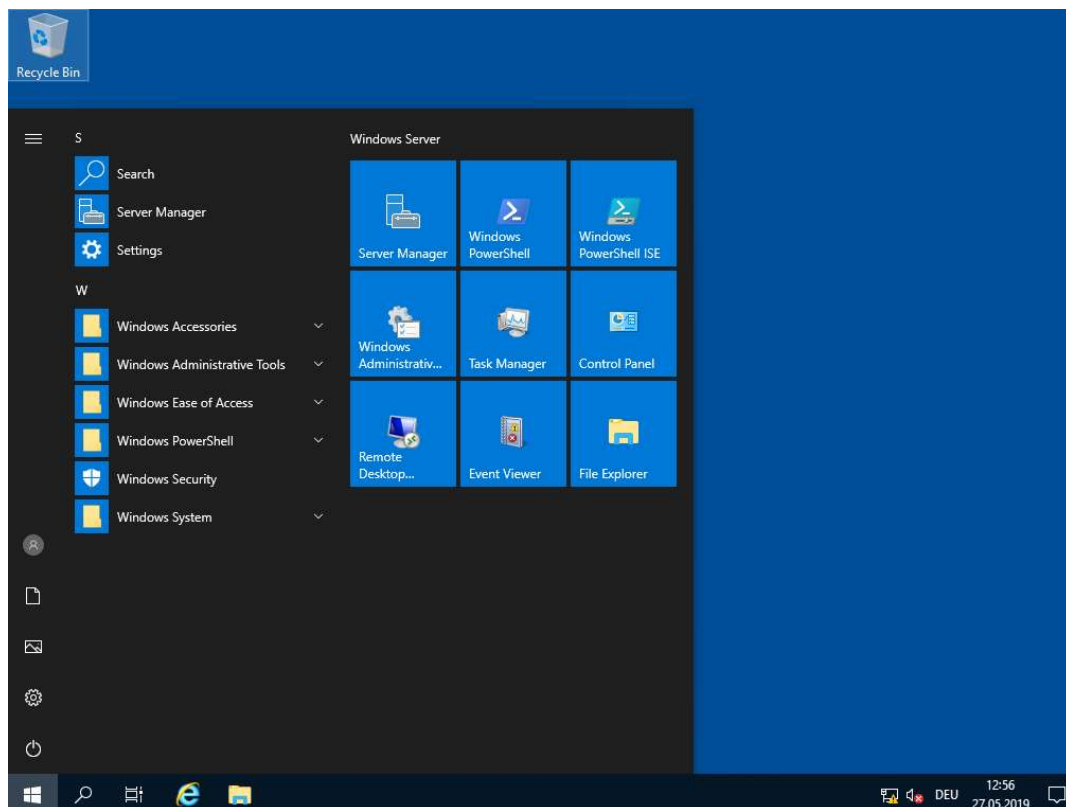


Figure 2. Windows Server 2016/2019. Looks like Microsoft Windows 10. (activedirectoryfaq.com)

The server was promoted to be able to act as a domain controller. New forest and domain were created. Forest is a forest of domains, a system where there can be multiple domains. If a domain controller will be retired, it must be demoted, both in case of a single domain controller being replaced and in case of one of multiple domain controllers

retiring. In older servers it was done often using “dcpromo” command in Command Prompt, but nowadays, through Powershell or using Server Manager to remove a role Active Directory Domain Services, which proposes to demote the Domain Controller, which should be done.

When demoting a DC, one makes it easier for everyone, because if its retiring and not demoted, later there will be issues for example with Group Policy, DNS and many other things, and the DC must be removed manually from multiple places, like DNS and as a Domain Controller from Active Directory Users and Computers.

Worst case is if the retired Domain Controller had Master Roles. These include Schema master, Domain naming master, PDC emulator and Infrastructure master. There is a query to retrieve the information about the roles, “netdom query fsmo”. It will tell which server has these roles. These roles should be transferred to a DC replacing the old one or to another DC.

When replacing an old Domain Controller with a new one, certain things must be considered. For example, Forest and Domain Functional levels. If you are migrating from Windows Server 2008 or 2012 r2 to Windows Server 2019, the minimum forest and domain functional levels must be 2008. In some environments, these functional levels are still 2003. It will not work to replicate the AD and SYSVOL to new DC before seeing these upgrades through. [4]

What also needs to be done, is to migrate FRS to DFSR. FRS stands for File Replication Service, which was a legacy way to replicate for example logon scripts and Group Policies from server to server. It is not supported in newer server operating systems. DFSR is the new way to do it, and it stands for Distributed File System Replication. In any case, the state of this migration should be checked even if the forest and domain functional levels are 2008. This is done by typing in CMD: “dfsrmig /getmigrationstate”. It should be eliminated in order to move forward. There are three types of migration.

Which migration to use depends on if the one migrating knows for sure that SYSVOL and everything else is intact. Also, it is possible that the one migrating does not know it but wants an option to rollback.

Migration is done with following commands: `dfsrmig /setglobalstate 1`. `Dfsrmig /getmigrationstate`. `Dfsrmig /setglobalstate 2`, if all domain controllers have migrated successfully to the Global state Prepared. Then the global state should be set to 3 if all domain controllers have migrated successfully to redirected.

Next it should be checked if they have migrated successfully to be eliminated. Before all these the correct security policy must be checked as well as multiple other things about consistency.

If you want the quicker migration, but you want the ability to rollback during the process, you do the same but without all the checks. If you do not need the ability to rollback, then you set the globalmigration state to 3, eliminated, without the first two steps.

Next DHCP preparation was done, the scope was created and activated. Scope is a range of IP-addresses to be assigned to the devices in the network. Also, a Default Gateway and DNS servers were defined of course as a primary DNS server the DC itself, to join workstations to domain, because the scope is for the domain network and this is a single server system. [5]

The File and Storage services were configured for file shares. Hiding the folders in a shared folder where the user does not have read permission into. Assigning quotas were necessary also to prevent users filling the available space, a certain amount of space was assigned per user.

2.2 Advancing in configuration

2.2.1 Certificate Authority

A new role was installed to Windows Server; certificate services to have a certificate authority. A certificate signing request was created and signed for the purpose of using it with NPS (Network Policy Server).

The certificate was manually installed on mobile devices, such as cell phones.

2.2.2 NPS

An additional role was installed on the Domain Controller, NPS for secure wireless authentication.

The connection policies were set up in NPS to use Active Directory Authentication per group if the RADIUS client IP matched.

2.2.3 AAD Connect

Azure Active Directory Connect was set up to synchronize between on-premises Active directory and Azure Active Directory. It has many advantages. For example, the password sync from local AD to cloud AD. Then Microsoft 365 user account passwords stay in sync with the domain passwords.

For this was added secondary User Principal Name suffix, with the domain information that was used in Microsoft 365. Then the usernames in Active directory could be changed to same form than email addresses, firstname.surname@domainname.fi, that they would sync with already created Azure AD accounts. Then the AAD Connect could be configured. Also, Single Sign On was added so that if a user was logged into a domain computer, they could easily and automatically login to Microsoft 365 in Microsoft Outlook and other services. [6]

New user accounts and groups were synced from local AD to cloud AD, as well as their passwords and user attributes.

Sometimes it seems, that the Microsoft 365 will use as email address a UPN (User Principal name, an attribute for username, which looks like email address) suffix of the tenant, .onmicrosoft.com, so the ProxyAddresses were set. SMTP in high case letters had to be used like SMTP:first.last@domain.fi in order to make it primary. Low case letters, smtp, would make it an additional one. Also, SIP: was used in ProxyAddresses for Teams. If additional attributes for email would be needed, such as hiding from global address list of the tenant, Schema in the local AD must be extended with Exchange schema. There is an attribute, which will be synced through AAD Connect to tell Exchange Online if to hide the user from the Global Address List. [7]

3 Network

This chapter focuses on a network that consists of TCP/IP networking with different network appliances and methods to connect the workstations remotely to the local area network.

3.1 Firewall

A firewall is a network security appliance or a network security software. A firewall can be a physical device that is meant and dedicated into firewall use that has a firewall software, or it can be a virtual computer with firewall software, or it can be a software inside an operating system of a computer which protects the computer from network attacks. In this, with firewall is meant a hardware device with a firewall OS.

A hardware firewall is placed as a gateway of a network to protect it from attacks. It is inspecting network traffic that originates from internet to local area network, or from local area network to internet. In past, firewalls were simple devices that allowed traffic out but no traffic in. [8]

Only traffic that was allowed in, was towards certain server and certain port. Nowadays firewalls are more complicated than that. They are deeply inspecting the traffic against malicious traffic signatures; they are scanning the traffic for viruses and they are decrypting encrypted traffic for inspection. Then they re-encrypt it using their own certificate, which should be placed to computers that it is protecting.

Firewall is also used to form a connection between different sites, for example from main office to branch office, often using internet connection but tunneling and encrypting the traffic. It is also used for remote working, through multiple different protocols. A client program in a workstation can tunnel and encrypt traffic to the office network through firewall.

To enhance cybersecurity of a network, it is recommended to use firewall logs to inspect the traffic, admin actions and system logs to go through things, in order to find things that automated inspection did not find. The logs can be used to troubleshoot connectivity issues, as well as finding traces of possible cyber-attacks.

3.1.1 Initial setup and introduction

Sophos XG 105 firewall was set up at main location. It was a good choice, because it is a next generation firewall with good support and services, it is a commercial firewall for small companies. For middle sized and enterprises, there are also firewalls from Sophos.

Sophos is a cybersecurity company from Great Britain, and it has listed well in tests against its competitors.[9]

Initial setup included registration of the firewall, license synchronization, which protection modules were taken into use and firmware update. WAN and LAN1 interfaces were configured. [10] See figures 3, 4 and 5 below.

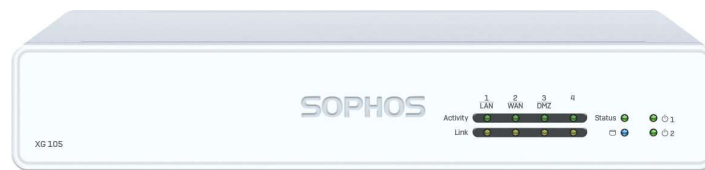


Figure 3. Sophos XG 105 Revision 3 front (avanet.com)

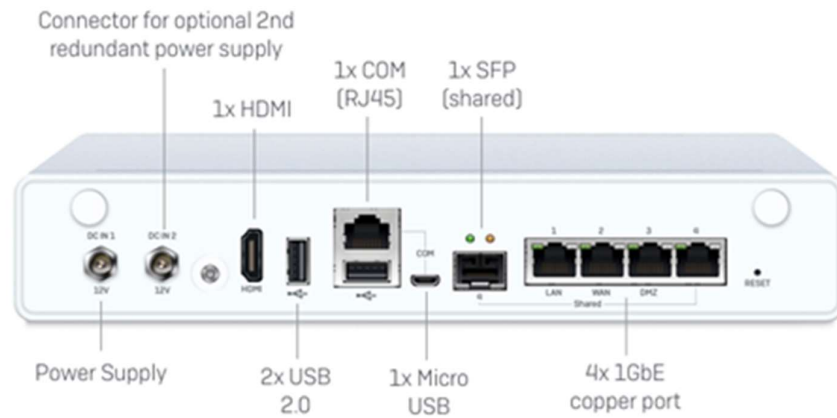


Figure 4. Sophos XG 105 Revision 3 back with information (snappernet.co.nz)

Figure 5. Sophos XG OS, 17.5 admin web portal. Simple and clean look. (avanet.com)

License chosen was Sophos XG FullGuard. EnterpriseGuard would be also good, but for a possibility to have a webserver in near future, FullGuard was chosen. Also, FullGuard includes Sophos Sandstorm, a Sophos cloud service where the suspicious files are sent for further inspection. [11]

Every possible protection module was selected. Firmware update was not performed, because the current version of the firmware had a bug which caused sometimes the firewall web configuration to crash, which led into a need of a factory reset. Because of this, the firmware had to be updated using the configuration website itself, not the initial setup.

The buggy default rule for SMTP protection was removed, because it caused issues in sending emails from the network.

Intrusion Prevention System (IPS) had a default configuration. This had to be customized because IPS rules inspection is a very resource hungry component. Only the parts which are needed in current installation, were selected. This is one of the components that makes a firewall good for modern use.

Firewall is just not an IP/Port filter that blocks certain IP addresses and ports from certain zones, but it has many ways to protect the network. IPS is a system that has a collection of signatures for malicious network traffic, compares it to current network traffic and if it matches with the signatures, it blocks/drops the traffic. [12]

Web proxy/filter had also a default configuration, which was not reasonable for this installation. Unneeded filters were removed and the ones needed were reconfigured. Web Proxy is a service protecting users while surfing internet. It could be configured also to limit the access to websites which are not categorized to be productive, or which are categorized criminal, for example.

Exceptions were a must because Office 365 installation and usability required some special rules. Special rules included disabling web proxy, Antivirus, Sandstorm and IPS for certain URLs. Ready exception pack could be downloaded from Sophos for O365 and it was imported to the firewall and enabled. In 17.x version of the firewall OS, without the exceptions many M365 functions were blocked, for example installation of the business

applications. In 18.x it is already fixed, so that the certain exceptions are ready and at background, not even showing up in exceptions list in which the exceptions can be enabled, disabled, and modified. Sandstorm is a good cloud sandboxing system, where the downloaded programs are automatically checked in cloud system before allowing the installation to download components from the internet, for example.

Traffic shaping was applied to preserve bandwidth for VoIP, such as Teams and Skype.

Next generation firewalls such as Sophos appliances, are very complex systems consisting of many different functions for protection of the network and connectivity.

Basic IPsec site to site and remote VPN tunnels, SSL VPN site to site and remote and some other protocols and clients are included. Also the appliances have wireless protection so that the firewall can be used as a wireless controller. You can add a RADIUS server as authentication source for wireless, add wireless networks, for example “separate VLAN” wireless SSID, “bridge to AP LAN” and “separate Zone”.

Bridge to AP LAN is simple. It needs just a LAN to LAN firewall rule in order to work. It is as if the clients of wireless access point would be part of the LAN network.

Separate VLAN is useful also in some cases, but separate Zone works also well, if you want to limit certain WLAN SSID traffic, for example that only the internet connection is allowed, but the traffic is isolated from the LAN. This is useful with a Guest WLAN, when you do not want the guests in a company or in a home network to access the private resources.

For separate Zone you need to either create a Zone or use existing Zone. Existing Zone to use is for example WLAN, but to leave the configuration simple and understandable, a Guest Zone can be created. Also, only certain services should be enabled for Guest Zone, but an access to the firewall administration portal and user portal for example should be left out for security. [13]

To use RADIUS for authenticating users of main SSID, you must choose it at the “Wireless Protection” tab, but first you must configure it as an authentication server at Authentication → servers.

If it is necessary to plan and build an enterprise level network with a main site (separate server room), the wireless access points at different sites can be configured to register with the main firewall in order to have a centralized administration.

A lot of work is needed, if one wants to configure the wireless networks separately to each appliance at different sites, when the access points can fetch their configuration from the main firewall only. In this case a site-to-site connection is needed.

IPsec is easy and works well, if the sites have static public IP address, but for those appliances that use DHCP to get their IP from the operator, Sophos provides an easy solution:

Sophos XG to Sophos XG RED connection (RED = Remote Ethernet Device).

To understand what needed to get the wireless AP to fetch their configuration from elsewhere than their local network, needs more knowledge than to use the graphical administration portal. For this, SSH connection for the local firewall is needed.

To fetch the configuration, wireless AP is going to try to contact a “magic IP”, 1.2.3.4. The firewall does not route it forward. For this, a DHCP option 234 must be created, as well as a static route to 1.2.3.4 using the RED interface as gateway, or with IPsec site to site, a tunnel route. [14]

If a remote site firewall uses an LTE module to connect internet, with 18.0.1 to 18.0.4 versions of the Firewall OS is a bug, that it does not create a default route. Also, the LTE interface shows an odd gateway IP. Creating a static route is a workaround. 0.0.0.0 is the destination IP address, with /0 netmask. Gateway IP field is left empty, and the interface chosen has to be the LTE interface.

This route must be “more expensive” than the magic IP, 1.2.3.4 route. The route needed with RED tunnel first routes traffic to 1.2.3.4 and to the remote site network, and only after, it routes traffic to everywhere else. Otherwise, it also routes 1.2.3.4 traffic and the remote site traffic through LTE interface, before it would try the other static route entries.

If there are problems, tcpdump in Advanced Shell through SSH connection is one of the best tools to resolve the issue.

3.1.2 Remote Access VPN

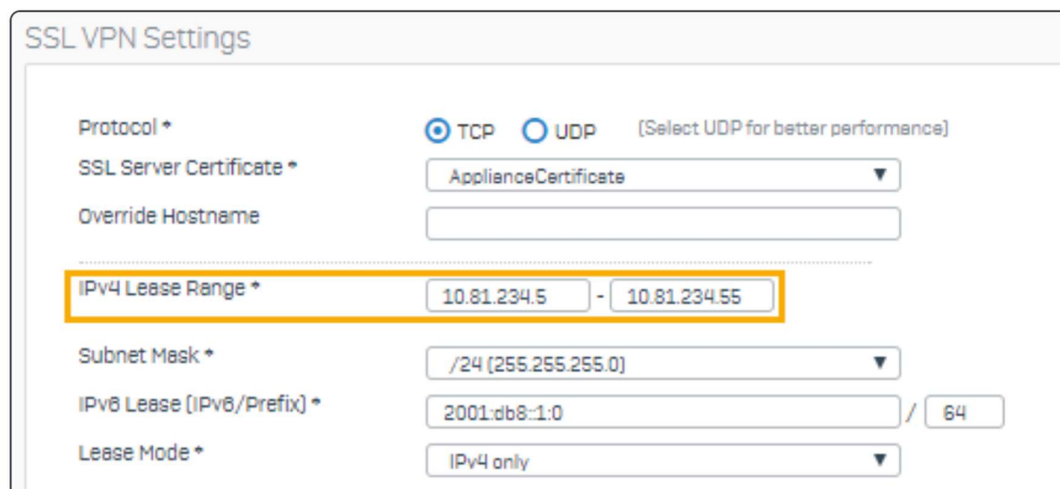
Remote access VPN is to allow connections from the internet to local area network safely and securely. Methods include SSL, IPsec, L2TP etc. This kind of connection is used in organizations in remote work to allow employees to access internal network resources, such as fileserver.

SSL VPN was chosen for this because of its quick and easy setup.

First, authentication had to be set up. Basic possibilities were local authentication and AD authentication. AD authentication was chosen over local authentication because with it there was no need to create extra user accounts. [15]

Server name, IP address, domain name, domain NETBIOS name, domain admin credentials, port number and search queries had to be told to the firewall in order to find user credentials for the firewall from AD. Port number was left to default.

Then the local subnet information and SSL VPN network had to be introduced to the firewall as variables. SSL VPN IP address range had to be configured.



The screenshot shows the 'SSL VPN Settings' configuration page. The 'IPv4 Lease Range' field is highlighted with a yellow box, indicating the IP address range for the VPN. The range is set to 10.81.234.5 - 10.81.234.55. Other settings include Protocol (TCP selected), SSL Server Certificate (ApplianceCertificate), Override Hostname, Subnet Mask (/24), IPv6 Lease (2001:db8:1:0), and Lease Mode (IPv4 only).

Figure 6. SSL VPN settings. (Sophos.com)

Figure 6 displays SSL VPN settings. Protocol TCP or UDP must be chosen. UDP has better performance because it is not “packet critical”, so it allows lost packets, which TCP does not. SSL server certificate, default is ApplianceCertificate.

This way the clients (with firewall generated client certificates) recognize the correct server and the certificates are used in encrypting the traffic. Overriding Hostname is not mandatory. It is used in cases where the firewall does not have a public static IP as their WAN interface IP, but when they are behind NAT and need to use dynamic DNS service.

IPv4 Lease Range is the range of IP addresses leased for the hosts that connect the SSL VPN networks. The hosts are recognized by this IP address and their MAC address, rather than using the local IP they have assigned in the local network they are connected to. Subnet mask defines the network size. IPv6 Lease has the default setting, but lease mode can be IPv4 only as in many cases as it is. See figure 7.

The screenshot shows a configuration form with the following fields and values:

- Name *: Local subnet
- IP version *: IPv4 IPv6
- Type *: IP Network IP range IP list
- IP address *: 192.168.0.0 Subnet: /24 (255.255.255.0)

Figure 7. Local subnet variable. (Sophos.com)

In SSL VPN settings and policy, as well as in firewall rule, these variables had to be selected for an access from VPN range and the VPN range had to be defined. User group with access to use SSL VPN had to be defined, and firewall rule created. [16]

Figure 7 shows an example variable. As in it can be seen, the type can be selected. Possible types are IP (address), Network, IP range and IP list. IP is a single IP address for a host, network is a full IP network, IP Range is from certain IP to certain IP and IP list can be different IP addresses in one variable instead of multiple variables with type IP.

The screenshot shows a firewall rule configuration interface. At the top, the 'Rule Name' field is set to 'Remote SSL VPN access' and is highlighted with an orange box. To its right is a 'Description' field with the placeholder text 'Enter Description'. Below the rule name, the 'Action' is set to 'Accept', with 'Drop' and 'Reject' options also visible. The 'Source' section contains two fields: 'Source Zones' set to 'VPN' and 'Source Networks and Devices' set to 'Remote SSL VPN range', both highlighted with orange boxes. Below these are 'Add New Item' buttons. The 'Destination & Services' section contains two fields: 'Destination Zones' set to 'LAN' and 'Destination Networks' set to 'Local subnet', both highlighted with orange boxes. Below these are also 'Add New Item' buttons.

Figure 8. Basic firewall rule for SSL VPN looks like this. (Sophos.com)

As seen in figure 8, adding a firewall rule can be very simple at basic level. This rule defines source and destination zones, networks/devices, and services/ports. [17]

SSL VPN zone is VPN, and Remote SSL VPN range (or network) is a variable which contains SSL VPN IP range or network, depending on the case. Figure 8 shows its range. Then destination zone is LAN, and destination network is Local subnet, a variable defined manually.

Figure 9. VPN policy settings. Basic settings. (Sophos.com)

Figure 9 shows the general settings for the SSL remote access VPN. Name field should be filled so, that it will be clear for other administrators later even if the network grows and needs different SSL VPN policies.

Policy members, in very small company, can be chosen “Open Group” which is a default group, or a newly created group like in the figure.

Tunnel Access, “use as default gateway” switch should be used carefully. It will forward ALL internet traffic to the SSL VPN tunnel, causing the traffic to go out through the fire-wall.

For security, it is a good thing, but it can cause different issues. For example, Microsoft modern authentication does not like this, because the modern authentication traffic tries

to go out through the original default gateway of the client computer and finds that there is no access to internet. It will not go through the VPN tunnel. In past, this could be fixed by forcing legacy authentication through regedit. The better way though was to add a static route to the Windows host for 0.0.0.0 (default route) to use the firewall IP as gateway, if the primary default gateway did not have connection. The latter works still.

In many cases it is better to not use the switch “use as default gateway” but to specify permitted network resources and add the newly created “local subnet” variable into it. This way, only the traffic sent to these IP addresses will use the VPN tunnel. Every other traffic will go to internet. Split tunneling is a good thing for performance, because traffic that goes to internet, goes directly, but the traffic destined to for example a company network, is protected. Though, an issue can raise from a situation, where a person uses open wireless networks to access sensitive company data in cloud or logging into their email and sending emails, when they travel and are for example in hotel or airport. Then this traffic is not protected by the firewall that protects the data that goes into the tunnel. This introduces a risk where an attacker in compromised network gains access to corporate computer using split tunneling, they also gain access to corporate network. If using full tunnel, then all the data goes through the VPN tunnel and is protected, and the firewall protects the normal internet traffic also. [18]

It is very important to notice that a subnet of any local network the client computer is connected, should not overlap with the SSL VPN network nor the “local subnet”, which is behind the firewall. This leads to routing issues.

For example, if an employee works from home, and their network IP address is the common 192.168.10.0/24, and the “local subnet” behind the firewall is also 192.168.10.0/24, and the VPN is connected, the client computer does not know where to send the traffic when trying to access server at 192.168.10.10. For example, it could try to send the traffic to a printer in the employee’s home network.

In a case like this, the network connections just do not work, so either the home network address should be changed, or the network behind the firewall.

In some cases, when many things already depend on this network behind the firewall, it might be easiest to change the home network IP address. But to plan the future, the best

is to change the networks IP address, that is behind the firewall, because it overlaps with the most common home network addresses. 192.168.0.0/24, 192.168.1.0/24, 192.168.10.0/24, 192.168.100.0/24 should be never used as company network addresses. If using 192.168.x.x networks at all, they should not overlap with the most common ones.

Authentication server for SSL VPN was selected to be the AD server defined earlier. Traffic quotas and limitations are set for a group if needed, in this case no quotas were assigned.

SSL VPN client application was downloaded from user portal, which can be reached using internet browser, and connecting to the firewall LAN IP from the local network, using https protocol. [19]

Then user had to log in with their AD username and password, download the client and configuration. Installing it needed minimum local admin rights. The configuration included user certificate.

After installation, an icon appeared next to the time and date in Windows, right bottom corner. Icon looks like a small traffic light, which has red light when offline, red, and yellow when trying to connect and green when connected.

It was also tested in a remote location that the user could connect and use the internal file server resources.

The SSL VPN which Sophos is using, is based on Open VPN. For mobile phone there is no Sophos SSL VPN client, so the Open VPN client had to be downloaded and from user portal the configuration file for it.

The connection worked also through phone, which could access the internal resources of file server and the security camera's live video stream.

3.2 RED

This chapter discusses a Sophos device, SD-RED. It is a device that performs a tunneled connection from a remote location to internal network. It is used for example in very small branch offices, construction yard offices etc. The tunneled connection is Software Defined. [20]

For remote location Sophos RED 15w was installed. It is information was used to set up a connection between it and the main location's firewall. See figures 10 and 11.

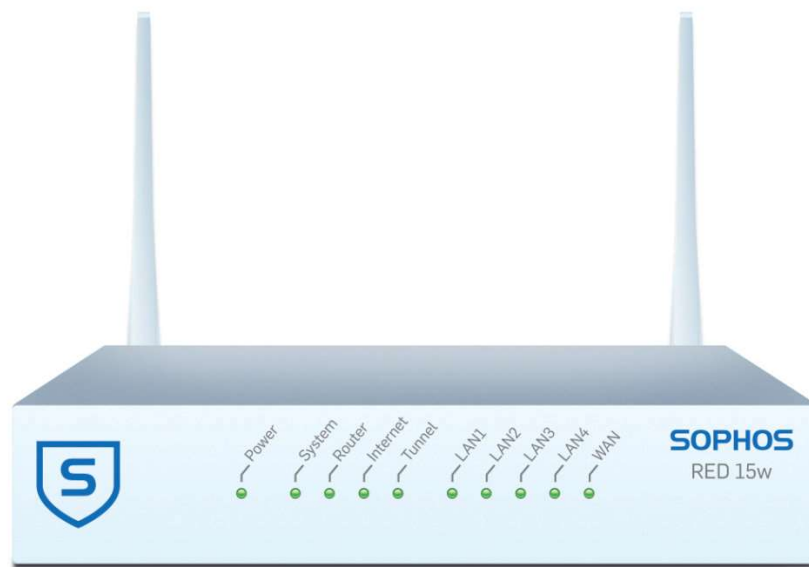


Figure 10. Sophos RED 15w frontside. (avanet.com)



Figure 11. Sophos RED 15w backside. (avanet.com)

The device has a lock code so it cannot be set up with another firewall without a lock code entered. Lock code was received through email to defined address.

The configuration was Standard/Unified mode so that all the connections will come first to the firewall and then to internet. The RED is connected to the remote location router, so all connections of all devices in remote location will pass through it. The firewall will work as DHCP server to provide the devices with IP addresses. [21]

Firewall was configured as a controller of RED 15w's integrated WLAN. The authentication of the RED's integrated WLAN was set to RADIUS, which is the AD server. That also means that WPA2 Enterprise was used.

3.3 Wireless Local Area Network (WLAN)

A company grade Zyxel Wireless Access Point was installed and set up to fetch settings from Zyxel Nebula cloud service, where the needed SSIDs were set up as well as connection with NPS installed on Windows Server. A secret key was needed, and IP of the server. The NPS had to be set up with same secret key and with the Zyxel Wireless

Access Point IP. The connection policies were set up in NPS (Network Policy Server) to use Active Directory Authentication per group, and to allow only connections from Zyxel Wireless AP. [22] See figures 12, 13 and 14.



Figure 12. This AP (NWA1123-ACv2) was used with the project. (Zyxel)

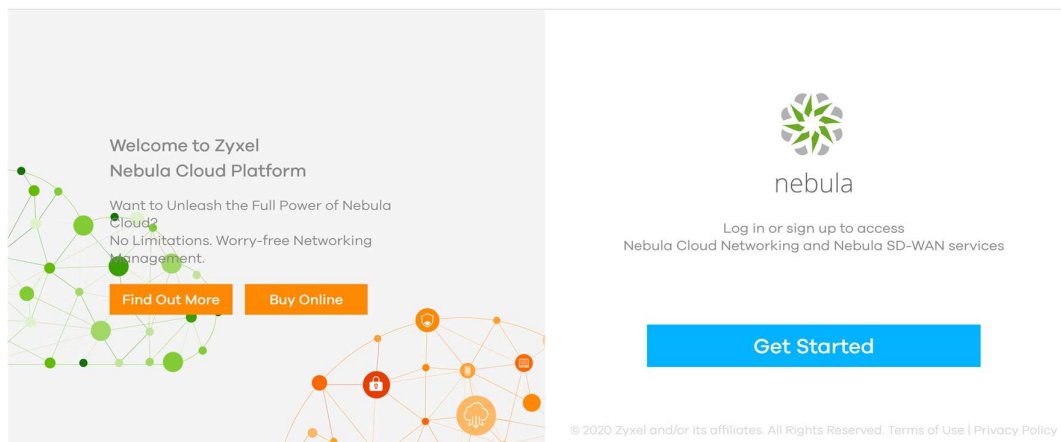


Figure 13. Zyxel Nebula Cloud first page. (nebula.zyxel.com)

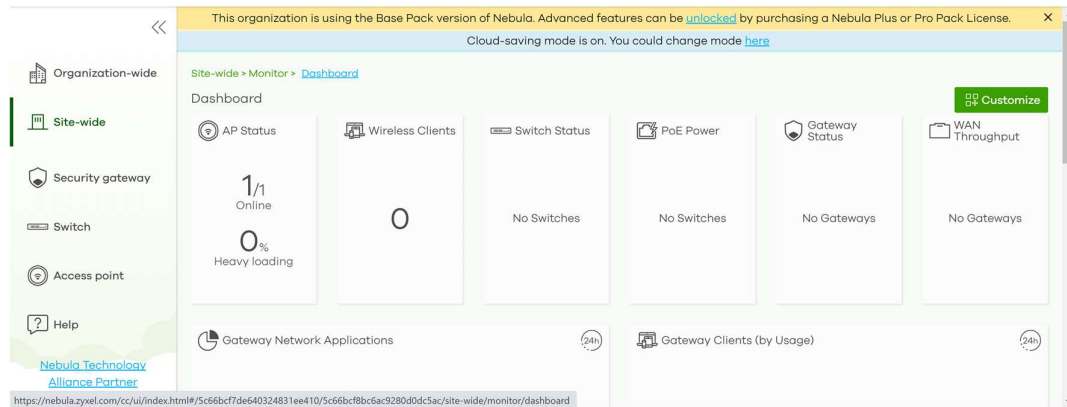


Figure 14. Zyxel Nebula Cloud, logged in. (nebula.zyxel.com)

Figure 14 shows Zyxel Nebula Cloud, a cloud management website for different Zyxel devices. In this case, it was used to configure the access point SSIDs and which server to use with RADIUS. Guest SSID authentication was configured to use a password + Facebook login after logging into the network. Guest network was isolated from other networks. Facebook login was added in order to identify the user of the network, it collected name and profile picture from users Facebook profile. This would make it more difficult for hackers to use this Guest network for illicit internet activities, because they would need to create a fake Facebook profile too.

NPS was set up to use that certificate and Group Policy was set up to deploy that certificate to the workstations.

3.4 Switching

A network switch is a must in modern computer network. It has multiple functions, for example to switch the traffic between interfaces and to prevent frame collision. [23]

One function could be to get rid of the need for crossover cables and replace them in future with cheaper patch cables (ethernet cables, with RJ45 connectors). Crossover cable would be needed for example if connecting two computers together.

A network switch forwards data using MAC addresses at the layer 2 of the OSI model. Some switches operate at layer 3, and then it is commonly called layer 3 (L3) switch. Then they are also able to route traffic in addition to switching.

L2 switch forwards traffic to a single device, instead of all of the devices connected to switch. Hub would forward it to all the devices. Therefore, even unmanaged switch has more intelligence than a hub.

OSI model is a commonly used model to make difference between different layers of network traffic. [24] See figure 15.

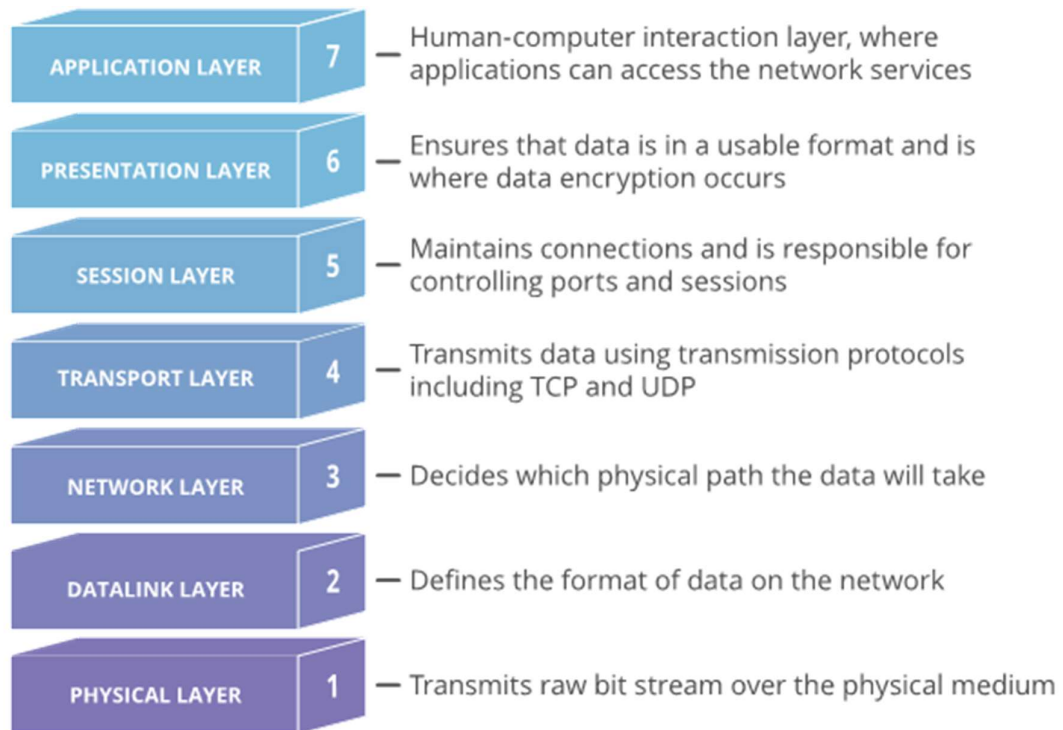


Figure 15. OSI-model. (cloudfare.com)

Ethernet interfaces (ports) are often used in commercial switches. Ethernet switches have one primary function: multiport layer-2 bridging. Layer-1 is a must in all switches because it supports the higher layers.

A switch can be a managed switch, which is way more expensive than non-managed switch. It provides such functionality for security that non-managed is not able to do. A non-managed switch is there just to switch traffic in its interfaces based on destination MAC addresses, but managed one brings in more security functions.

For example, in management interface, one can lock certain interfaces (ports) that only certain MAC addresses get through it, thus limiting possibility for non-company computer being connected into the network by a hacker for malicious purposes. Also, certain ports can be completely closed from use.

Switches come in many sizes for different purposes. There are ways to categorize them: managed and non-managed, desktop switch and rack switch, categorizing them by number of ports and port types, PoE or non-PoE, Gigabit, RJ45 only or some SFP ports too in it etc. [25] See figures 16 and 17.



Figure 16. A rack mounted 24-port 3Com ethernet switch. (commons.wikimedia.com)



Figure 17. 5-port ethernet desktop switch. (commons.wikimedia.com)

This current project does not use any of the switches in photos. It uses another kind of 5-port gigabit desktop switch.

4 Workstations

Domain workstations are client computers joined to Active Directory Domain. They are used as work computers of employees and leadership. In this case they are personal computers, which are also used for working. They receive company policy from Active Directory Domain Controller. [26]

Windows 10 Education was installed to the workstations. Workstations included a desktop computer with Intel Core i7, 16 GB of RAM, MSI GeForce GTX 1080, M.2 PCIe SSD 256 GB, 500 GB 2.5" SSD, 1 TB HDD, PCIe WLAN and a laptop computer with Intel Pentium, 8 GB of RAM, 2.5" SSD and integrated graphics card.

After basic installation they were joined to AD domain. After first user login they fetched the Group Policy configuration, certificates, mapped network drives, printer etc. from the Domain Controller, which also had different roles in this situation, while often multiple servers are used to perform different roles and for redundancy. [27]

Both computers were able to connect to WLAN with AD credentials. They were also able to connect devices at another location where the RED was installed at. The devices at remote location were able to connect the main location devices, and the WLAN SSID provided by the firewall, using AD credentials. See figure 18.

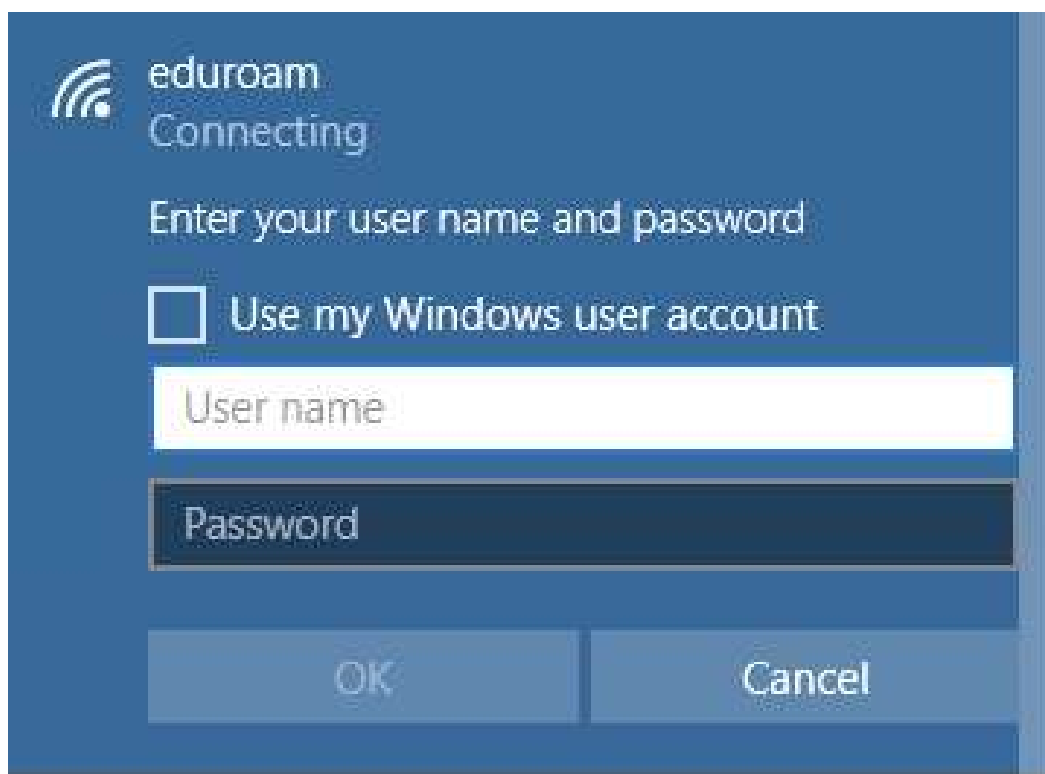


Figure 18. Credential request of enterprise network, like PEAP-MSCHAPv2 as in the project. (wireless.csu.edu.au wireless support pages)

5 Microsoft 365

5.1 Licensing

When the users from on-premises AD were synced to the Azure AD with their attributes, the licensing was done. In this, it was done by assigning the licenses manually to users. Microsoft 365 Business Premium was used (earlier Microsoft 365 Business).

In a larger environment, where everything is automated, should be used a system where administrator adds groups in local AD for the licenses, for example O365_E3, M365_E3 etc. for Office 365 Enterprise E3 and M365 Enterprise E3, respectively, and AAD Connect would sync those groups and information of users in them. [28]

Users should be added to these groups depending on the license they need. In Azure AD, there is a menu for licensing. There can be added certain license to certain group – then the license is automatically assigned to users in certain group. See figure 19.

The minus in this is that, that then there should be free licenses all the time, which would grow unnecessary expenses. Of course, there could be some volume license, but for 365, Microsoft does not sell them anymore.

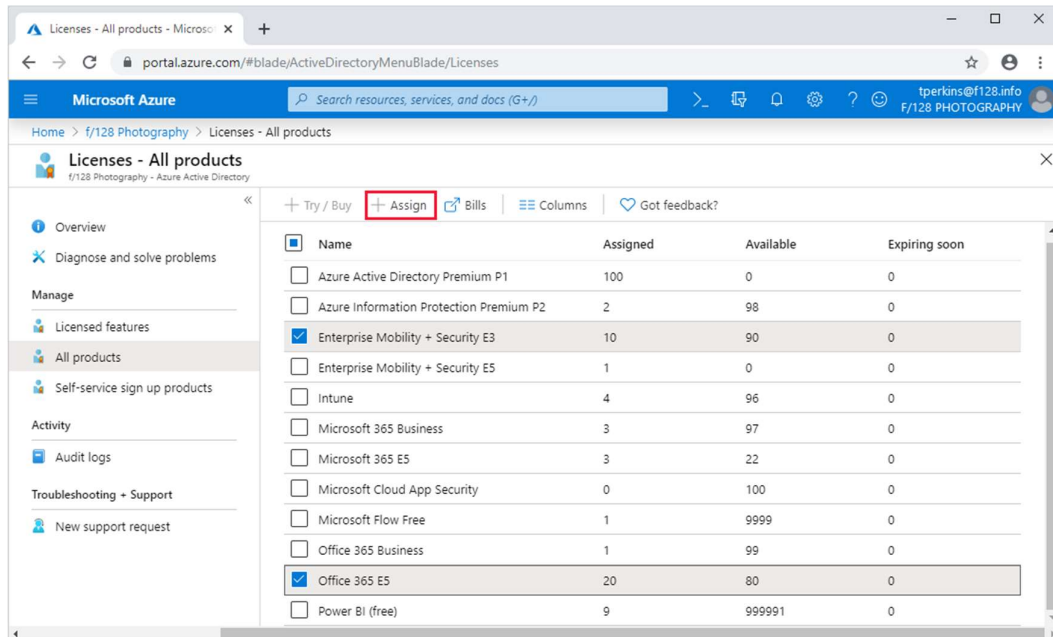


Figure 19. Assigning licenses to a group. (docs.microsoft.com)

Microsoft 365 Business Premium was chosen for this because it has the needed desktop applications, mailbox of 50 gigabytes, possibility to send Microsoft 365 encrypted emails (mainly Encrypt only and Do not forward were used), and possibility to add some security through Security Center. [29]

Enhanced phishing protection, spam protection and protection against pretending someone else were taken into use. The advanced security could be added to other licenses by buying extra license, called Microsoft Defender for Office 365.

5.2 Intune and Endpoint Management

Endpoint Manager is a cloud-based management tool by Microsoft. It brings Endpoint analytics and management for devices, such as workstations and mobile devices. Endpoint Manager and Intune is managed using web browser. Intune is a part of Endpoint Manager. [30]

Endpoint Manager was set up to install PDF reader and to apply some policies, like forcing BitLocker for encrypting the System drive. Intune Company Portal was forced to install to workstations and mobile. Mobile policies were added, such as forced screen lock. To Domain Group Policy was added a policy that forces enrollment to Intune. See figure 20.

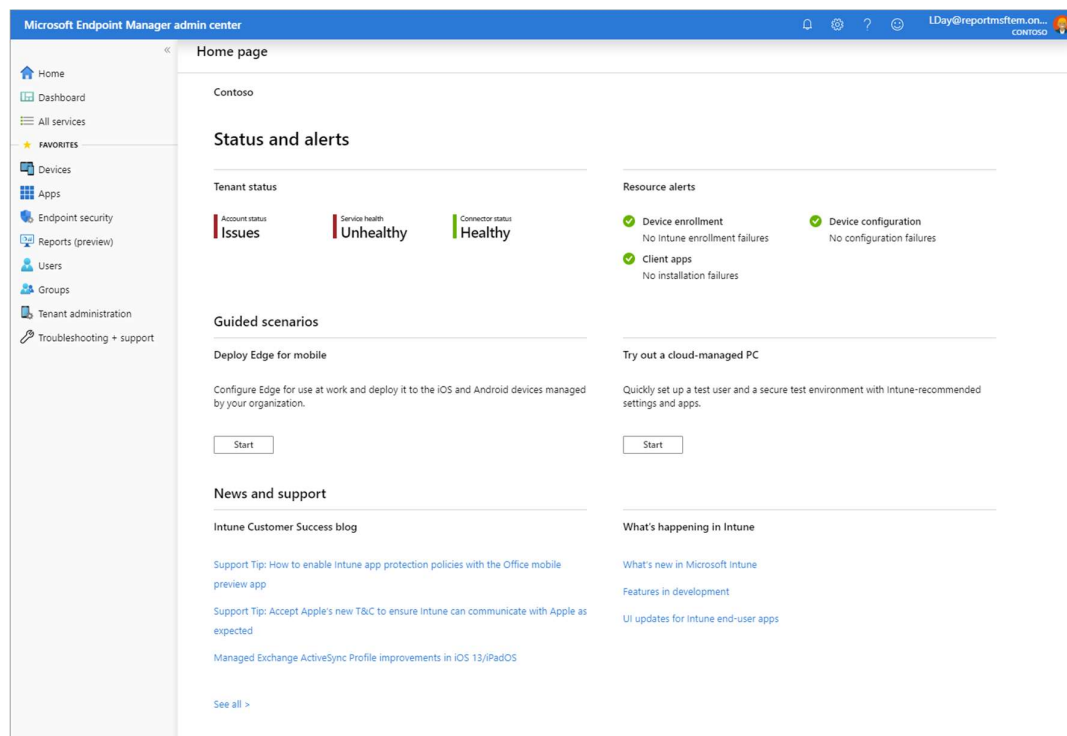


Figure 20. Endpoint management. (docs.microsoft.com)

There are multiple addons for Endpoint Management/Intune, provided by third parties. Some are for endpoint analytics only, some are for controlling Intune and some are for

both. For example, Finnish RiihiDMA by RiihiCloud, has both. They provide the ability to deliver Smart Packets, as they call them.

There are policies, like forcing BitLocker, adding desktop icons, removing old Flash Player etc. There are also push installs. [31]

There are many push install packets ready, which are general programs in use by many companies. There is also a possibility to send them an installer of some custom or rare program, which they will make into a packet that can be installed easily using Intune.

You could take for example a licensed virus killer, and they would make it to install with your license. Or licensed TeamViewer Host and custom settings for it.

They also listen to request, one of the latest request made true was fetching a Teamviewer ID of Endpoint to their system so that when you go to check the list of endpoints they fetch from Intune, and click on certain endpoint, you can see their Teamviewer ID.

6 Conclusion

The purpose of this study was to create a company like network at home. This setup needed a long time for planning, studying, and working on, but it was worth all it. There were difficulties, especially with NPS. Finding a right policy was not as easy as in different instructions. Different instructions were tried without help. However, using them in combination with some troubleshooting helped. Domain member computers were easier, because the certificate could be distributed through Group Policy, but mobile devices needed the certificate to be installed into them.

Firewall LAN ports did not work similarly to switch ports if not bridged, they needed a LAN to LAN rule, to allow traffic between them.

With security camera, there was some pondering whether to add security or simplicity. Security was chosen, by disabling a protocol for easy use, and VPN was used to watch the live video.

Distributing applications using Group Policy was somewhat difficult. Using built-in Group Policy to distribute apps needed .msi files, not .exe files as installers. Some apps had them already, whereas some had to be wrapped into .msi. Instead of wrapping, logon script was a good choice, even though it seemed slower. [32]

In conclusion, it became clear that doing this kind of setup for a company like network helps to learn a lot about troubleshooting. Using time and effort will certainly help to set up an easier system later. It will need a lot of work to keep up to date but based on this study, it would probably be worth of effort and money in companies with more than five employees minimum.

References

- 1 Microsoft, Active Directory Domain Services Overview, Read 9 October 2021
<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>
- 2 Microsoft, Active Directory Security Groups, Read 9 October 2021
[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn579255\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn579255(v=ws.11))
- 3 Microsoft, Dynamic Host Configuration Protocol (DHCP), Read 9 October 2021
<https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top>
- 4 RebelAdmin, Step-by-Step Guide: Active Directory Migration from Windows Server 2008 to Windows Server 2019, Read 9 October 2021
<https://www.rebeladmin.com/2020/08/active-directory-migration-from-windows-server-2008-to-2019/>
- 5 Microsoft, How To Install and Configure a DHCP Server in a Workgroup, Read 9 October 2021
<https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/install-configure-dhcp-server-workgroup>
- 6 Microsoft, Custom installation of Azure Active Directory Connect, Read 9 October 2021
<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom>
- 7 Jack Stromberg, How to hide users from the GAL in Office 365 synchronized from on-premises, Read 9 October 2021
<https://jackstromberg.com/2018/08/how-to-hide-users-from-the-gal-in-office-365-synchronized-from-on-premises/>

- 8 Cisco, What Is a Next-Generation Firewall, Read 9 October 2021
<https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html>
- 9 Gartner, Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls), Read 16 October 2021
<https://www.gartner.com/technology/media-products/newsletters/sophos/1-5GVMBMU/gartner.html>
- 10 Sophos, Sophos Firewall v17: Registration & Setup Wizard, Read 9 October 2021
<https://techvids.sophos.com/watch/zYjM546vVi3MjWynbWerx2>
- 11 Sophos, Sophos Sandstorm, Read 9 October 2021
<https://www.sophos.com/en-us/lp/sandstorm.aspx>
- 12 Sophos, IPS, Read 9 October 2021
<https://docs.sophos.com/nsg/sophos-firewall/v17.0.0/Help/en-us/webhelp/onlinehelp/index.html#page/onlinehelp/IpsPolicyManage.html>
- 13 Sophos, Next Steps for Separate Zone Networks, Read 9 October 2021
<https://docs.sophos.com/nsg/sophos-firewall/v17.0.0/Help/en-us/webhelp/onlinehelp/index.html#page/onlinehelp%2FWPNetworkManageSeparateZone.html%23>
- 14 Sophos, How to troubleshoot registration issues for the Sophos Access Point, Read 9 October 2021
https://support.sophos.com/support/s/article/KB-000034799?language=en_US
- 15 Sophos, Configuring Active Directory authentication, Read 9 October 2021
<https://docs.sophos.com/nsg/sophos-firewall/17.5/Help/en-us/webhelp/online-help/nsg/sfos/learningContents/ConfiguringActiveDirectoryAuthentication.html>

- 16 Sophos, Sophos Firewall: Configure SSL VPN remote access, Read 9 October 2021
https://support.sophos.com/support/s/article/KB-000035542?language=en_US
- 17 Sophos, Creating a remote access SSL VPN, Read 9 October 2021
<https://docs.sophos.com/nsg/sophos-firewall/17.5/Help/en-us/webhelp/online-help/nsg/sfos/learningContents/CreatingRemoteAccessSSLVPN.html>
- 18 Kevin Dooley, The Pros and Cons of VPN Split Tunneling, Read 9 October 2021
<https://www.auvik.com/franklyit/blog/vpn-split-tunneling/>
- 19 Sophos, Create Remote Access SSL VPN, Read 9 October 2021
<https://docs.sophos.com/nsg/sophos-firewall/18.5/Help/en-us/webhelp/online-help/nsg/sfos/learningContent/VPNCreateRemoteAccessSSLVPN.html>
- 20 Sophos, Sophos SD-RED, Read 9 October 2021
<https://www.sophos.com/medialibrary/pdfs/factsheets/sophos-sd-red-ds.pdf>
- 21 Sophos, Sophos Firewall: RED (Remote Ethernet Device) technical training guide, Read 9 October 2021
<https://support.sophos.com/support/s/article/KB-000036699>
- 22 Microsoft, Network Policy Server (NPS), Read 9 October 2021
<https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-top>
- 23 CC Expert, Collision Domains and Switch Buffering, Read 9 October 2021
<https://www.ccexpert.us/routing-switching/collision-domains-and-switch-buffering.html>
- 24 Cloudflare, What is the OSI Model, Read 9 October 2021
<https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/>

- 25 Fortinet, What is an Ethernet Switch, Read 9 October 2021
<https://www.fortinet.com/resources/cyberglossary/what-is-ethernet-switching>
- 26 Microsoft, Applying Group Policy, Read 9 October 2021
<https://docs.microsoft.com/en-us/previous-versions/windows/desktop/policy/applying-group-policy>
- 27 Microsoft, Failover Clustering in Windows Server and Azure Stack HCI, Read 9 October 2021
<https://docs.microsoft.com/en-us/windows-server/failover-clustering/failover-clustering-overview>
- 28 Microsoft, What is group-based licensing in Azure Active Directory, Read 9 October 2021
<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-licensing-what-is-azure-portal>
- 29 Microsoft, Microsoft 365 Business Premium, Read 9 October 2021
<https://www.microsoft.com/en-us/microsoft-365/business/microsoft-365-business-premium?activetab=pivot%3aoverviewtab>
- 30 Microsoft, Microsoft Endpoint Manager, Read 9 October 2021
<https://www.microsoft.com/en-us/security/business/microsoft-endpoint-manager>
- 31 Riihicloud, Riihicloud front page, Read 9 October 2021
<https://riihicloud.com/>
- 32 Microsoft, Use Group Policy to remotely install software, Read 9 October 2021
<https://docs.microsoft.com/en-us/troubleshoot/windows-server/group-policy/use-group-policy-to-install-software>