Infrastructure Design

Technical Design for Network infrastructure on Barenbrug project

Document details

Version: V 1.0
Status: Approved
Last Updated: 05-Oct-20
Author: Alexey Protchenkov

CHECK REGIONAL REQUIREMENT FOR THE FOLLOWING WORDS:

Accuracy: Fujitsu endeavours to ensure that the information contained in this document is correct but, whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.

Non-disclosure: The information contained in this document is confidential and is submitted by Fujitsu on the basis that the customer will use it solely for the purposes of evaluating Fujitsu's design. The customer may permit those of its employees, advisers and agents having a need to know the contents of this design to have access to such contents, but shall ensure that such employees, advisers and agents are bound by the customer's obligation to keep it confidential. Subject to that, the contents may not be disclosed in whole or in part to any third party without the prior express written consent of Fujitsu. The customer's acceptance of these obligations shall be indicated by the customer's use of any of the information contained in this document.

Contents

Contents 2

Section A – Infrastructure Design - High Level 4

1. Introduction & Background 4

1.1 Purpose & Relationships 4
1.2 Scope & Requirements 4
1.3 Low Level Designs and Offerings 4

2. Risks, Assumptions, Issues, Dependencies and Constraints 6

2.1 Risks 6
2.2 Assumptions 6
2.3 Issues 7
2.4 Dependencies 7
2.5 Constraints (Standards, Policies, Guidelines) 7

3. High Level Design 8

3.1 Design Overview & Description 8
3.1.1 Global WAN configuration 8
3.1.2 LAN physical configuration 8
3.1.3 LAN logical configuration 10
3.2 Design Decisions 10
3.3 Impact on Existing Infrastructures 11
3.4 Decommissioning 11
3.5 Interoperability & Integrations 11
3.6 Test & Validation 11

4. Non-Functional Requirements Approach 12

4.1 Availability & Resilience 12
4.1.1 Backup and Restore 12
4.2 Capacity and Performance Management 12
4.2.1 Sizing Assumptions 12
4.2.2 Customer Data 12
4.2.3 Growth and Sizing (Current and Future) 13

5. Enterprise Management & Supportability 14

5.1 Remote Support 14
5.2 Monitoring 14

6. Security, Compliance & Data Map 15

6.1 Security 15
6.2 Compliance 15
6.3 Data Map 15

Section B – Infrastructure Design - Low Level 17

7. Naming and numbering convention 17

7.1 Location list and naming 17
7.2 Device naming 17
7.3 IP-addresing 17
7.4 VLAN-numbering 19

8. Detailed network configuration 21

8.1 Cisco MX configuration 21
8.1.1 General information 21
8.1.2 VLAN configuration 21

8.1.3 WAN and Internet connection 21
8.1.4 VPN configuration 21
8.1.5 Routing at central hub 22
8.1.6 Address translation 22
8.1.7 Traffic filtering 22
8.1.8 DHCP and DNS service 22
8.1.9 Logging and monitoring 22
8.2 Cisco MS configuration 22
8.2.1 General information 22
8.2.2 VLAN configuration 22
8.2.3 Spanning tree configuration 23
8.3 Cisco MR configuration 23
8.3.1 General information 23
8.3.2 Mode of operation 23
8.3.3 Authentication and encryption 23
8.4 Physical Components Placement 23
8.5 Code of Connection 23
8.6 Bill of Materials 24
Section C – Appendices as Required 26
9. Glossary of Terms 27
10. Document Control 28
11. Change History 29

Section A – Infrastructure Design - High Level

1. Introduction & Background

Barenbrug is about to implement new unified network infrastructure for its offices worldwide.
This document provides High and Low level Design for network solution for Barenbrug.

1.1 Purpose & Relationships

Related Documents	Status	Link
AOD		
TAD		
etc.		

Target Readership	Role
Name	In the project
Name	
Name	

1.2 Scope & Requirements

Ref	Requirement	Source	Req Met (Y/N)	Action taken
REQ001	New green field network design has to be developed for Barenbrug			
REQ002	Network design will be based on best practice with very limited information regarding existing network infrastructure			
REQ003	No migration of existing infrastructure is required in this design			
	To be updated			

1.3 Low Level Designs and Offerings

Offerings	Description	Link
Name		

Low Level Design	Description	Link

Name		

2. Risks, Assumptions, Issues, Dependencies and Constraints

2.1 Risks

Risk	Phase	Risk Description	Risk Containment	Fall-back	Impact	Prob.
RISK001		Single point of failure is one Cisco Meraki virtual appliance in Azure. If its fails Azure will be totally not available for customer				
RISK002		No network redundancy at customer locations. If network gear or Internet circuit is down, no access to cloud hosted services or Internet				

2.2 Assumptions

Ref.	Assumption	Impact if false	Actions
ASMP001	Green field network design has to be developed for Barenbrug		
ASMP002	Network design will be based on best practice with very limited information regarding existing network infrastructure		
ASMP003	No migration of existing infrastructure is required in this design		
ASMP004	Network functionality required is supported by chosen equipment		
ASMP005	Wi-Fi radio coverage review is out of scope, WAPs mount location is a local team responsibility		
ASMP006	Barenbrug security specific settings are considered as out of scope		
ASMP007	Redundancy is not foreseen as part of design for Azure or branches		
ASMP008	QOS for WI Fi is out of scope		
ASMP009	Internet connection is available at company locations for Cisco Meraki equipment configuration	Meraki configuration can not be pushed to network devices. No Internet connection testing and VPN can be performed for Meraki equipment	

2.3 Issues

Ref	Issue	Action
IS001	No complete overview of current environment which may lead to unforeseen design requirements	Provide due-diligence questionnaire to customer and collect input

2.4 Dependencies

Ref.	Dependency	Dependency on	Impact if not fulfilled
DEPD001	At lease one port from local ISP will be available for Meraki MX device connection to Internet		

2.5 Constraints (Standards, Policies, Guidelines)

Ref.	Dependency	Source	Impact if not fulfilled
CSTR001	To comply with GDPR	Client & Fujitsu	Potential legal action

3. High Level Design

3.1 Design Overview & Description

Barenbrug will deploy unified network solution in its all locations worldwide. Solution is based on Cisco Meraki product family. Following sections describe solution in detail.

3.1.1 Global WAN configuration

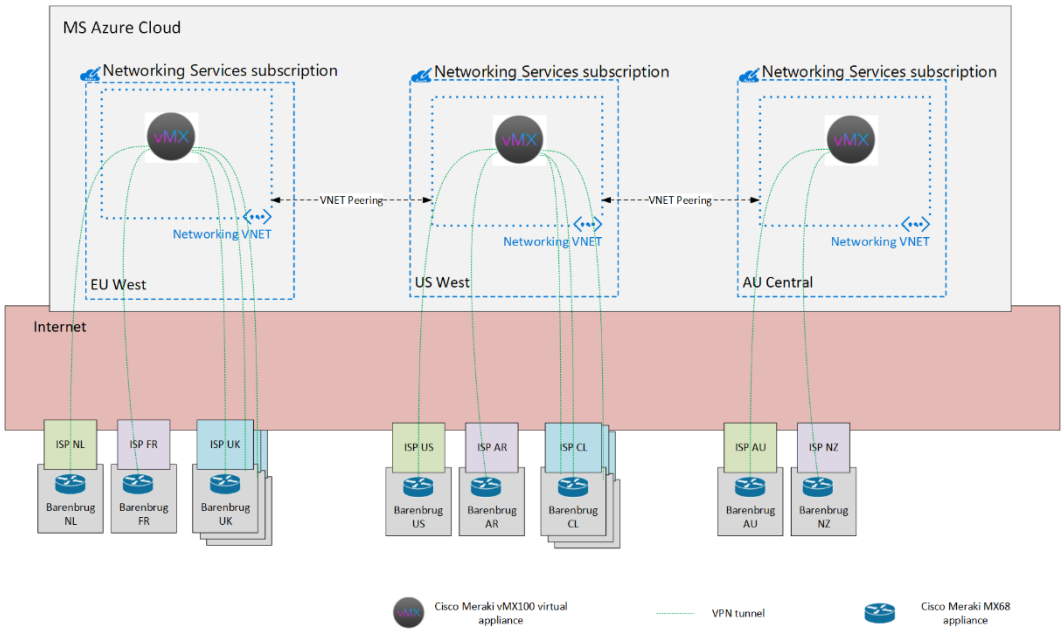
Barenbrug global network topology will follow multi-hub and spokes model. Where hubs will be located at Microsoft Azure public cloud sites with Cisco Meraki virtual appliance deployed as VPN terminating device. Each Barenbrug physical office location will be acting as a spoke and have VPN connection initiated by local Cisco Meraki MX appliance to one of the hubs.

VPN connections will be using Internet lines as transport for encrypted communications. VPN tunnel will be initiated and terminated on Cisco Meraki MX security appliances. Every location will have VPN tunnel to hub. If connection to primary Hub fails for some reason, it will be rerouted to another hub in different location. Hubs will aggregate and terminate VPN connections from remote sites.

There will be no redundancy neither on hub sites nor on spokes. Every site will be using single Cisco Meraki MX security appliance and single Internet connection. In case of failure of either equipment or Internet connection, communication within the site or to outside would be affected (depends on type of failure).

Logical diagram of hub and spoke connection model for Barenbrug is represented on figure below.

Figure 1 Global WAN topology



3.1.2 LAN physical configuration

From physical topology prospective every location network consists of aggregation layer firewall, access layer switches, and wireless access points. For extra small locations though these layer are collapsed into one.

Aggregation firewall is connected to Internet circuit provided by local ISP (Internet Service Provider) using copper interface. Access switches are connected to aggregation firewall using UTP cables. Wireless access points are connected to access switches using UTP cables.

There will be four types of Barenbrug locations depending on number of users at location:

- Extra Small
- Small
- Medium
- Large

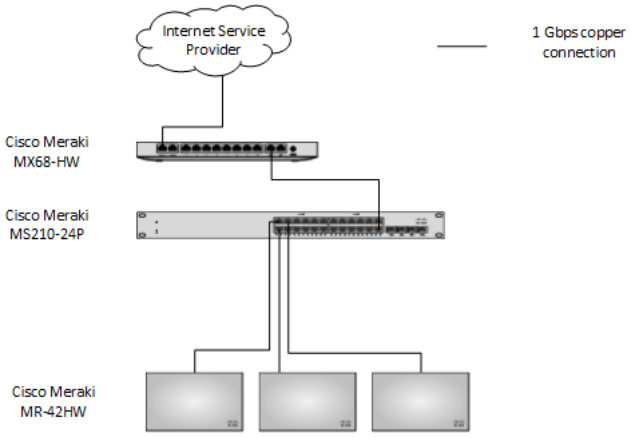
Every company location will have similar network topology. But number of access switches, wireless access points (WAPs) and Cisco Meraki MX appliance model may be different on different type of sites. Hyper-V servers will be hosted locally on medium and large sites.

Extra Small site physical diagram is shown below.

Figure 2 Extra Small site network layout

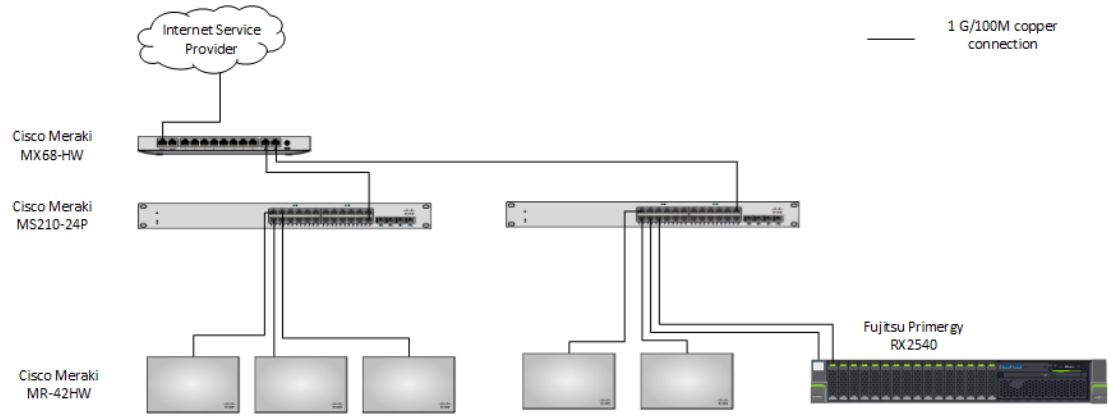
Small site physical diagram is shown below.

Figure 3 Small site network layout



Medium site physical diagram is shown below.

Figure 4 Medium site network layout



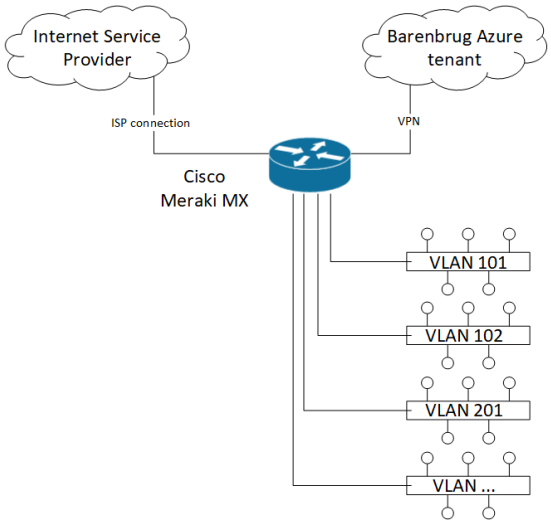
3.1.3 LAN logical configuration

Logically site consists of number of VLANs which are terminated on security appliance. Access switches are acting as L2 devices.

VLAN numbering follows single scheme for every site. VLAN numbers are locally significant and can overlap across sites. VLAN numbering scheme is provided in LLD section.

Site logical diagram is shown on picture below.

Figure 5 Branch logical network layout



3.2 Design Decisions

Decision	Rationale
Barenbrug global WAN network will be using hub and spoke communication model. Hub will be located at Microsoft Azure public cloud. All Barenbrug office/warehouse locations will be acting as spokes.	This is simplified and best practice topology makes design clear for understanding and management. While keep it functional and flexible for extra needs in future
Similar architecture and set of hardware will be used for each physical location	Network can be easily extended by adding new pieces of equipment. No significant changes in topology or redesign needed. Single blueprint provides easy management, shorter implementation times, shorter fault resolution

	times. One network vendor provides maximum compatibility, access to features, single management and monitoring
Cloud managed network devices will be used	Single configuration console and unified interface for all devices provide simplified management, shortened implementation times.
Remote access VPN will be used for teleworkers and remote users to get access to company internal resources	This gives users ability to remotely access company resources not only from office locations, but from any location with Internet access.

3.3 Impact on Existing Infrastructures

New network infrastructure for Barenbrug will be built as green field project, sitting next to existent, no impact is foreseen on existing network.

3.4 Decommissioning

No decommissioning is foreseen as part of this project

3.5 Interoperability & Integrations

Barenbrug network deployment project is considered as green field and equipment will be deployed next to existing Barenbrug infrastructure. Its not planned that existing network infrastructure will somehow impact on new one or vice versa.

3.6 Test & Validation

Following tests will be performed at every location after network deployment and configuration.

Test name	Test details
Basic network equipment validation.	All network equipment is powered on with no visible damaged, front/back panel alarms, log errors. It's basically functional and accessible remotely.
Basic network configuration	Network equipment is configured with basic settings like hostname, IP-addresses, Vlans, SSIDs.
Basic connectivity	Wired or wireless client connects to switches and APs and acquires correct IP-configuration
Internet connectivity	Client connected to the network can access Internet resources
VPN connectivity (local site to Azure VPN testing)	Client connected to local network equipment can access Azure based resources withoun running any VPN software at end client

4. Non-Functional Requirements Approach

4.1 Availability & Resilience

Network service availability relies among other on hardware redundancy which is not implemented in Barenbrug project. Security appliances at physical locations are installed one per site. In case of hardware failure, gear need to be replaced by vendor, which is provisioned by respective support contracts. During repair Internet access and VPN access will not be available to end users of this location.

In case of network software failures service interruptions are also possible depending on failure types. Support engineer remote intervention may be required in order to restore service.

Cloud virtual appliance are also deployed in non-redundant way. In case of underlying hardware failure on cloud service provider site, support engineer intervention may be required to restore service. VPN hub failure will affect number of locations within region in regards of VPN connectivity and access to central services.

4.1.1 Backup and Restore

Network configuration backup is implemented by Cisco Meraki cloud software. Current configuration is automatically saved in cloud. If snapshot of current configuration need to be done before implementing change, then it can be cloned to another dummy device or organization within Cisco Meraki dashboard.

4.2 Capacity and Performance Management

4.2.1 Sizing Assumptions

Sizing assumptions were made based on Barenbrug input of number of end users at every location. Its assumed that most of end users will be using wireless connections. Common practice is to estimate not more than 30 wireless users per one access point with no excessive traffic load.

Following table shows numbers of planned users per site vs average wireless network capacity:

Site sizing	Max number of users	Max capacity
Extra Small	under 20	1AP*30users/AP
Small	under 50	3AP*30users/AP=90 users
Medium	60	5AP*30users/AP=150 users
Large	120	5AP*30users/AP=150 users

Wired local network provides capacity of 1Gbps for fast access to local resources.

Internet connectivity is dependent of local contracts with ISPs and is not within scope of this design.

At cloud locations virtual appliance vMX will be deployed

4.2.2 Customer Data

Customer data migration is out of scope of current project.

4.2.3 Growth and Sizing (Current and Future)

Proposed solution capacity is will over current demands and can be scaled by adding more network ports or wireless access points. ISP connection can be extended over time if needed.

5. Enterprise Management & Supportability

5.1 Remote Support

Remote support of Cisco Meraki devices will be organized via Meraki cloud dashboard, centralized, web browser-based tool used to monitor and configure Meraki devices and services.

5.2 Monitoring

Meraki device monitoring is provided via Meraki cloud dashboard tool, web browser-based tool used to monitor and configure Meraki devices and services.

6. Security, Compliance & Data Map

6.1 Security

This document provides the following operational security service components:

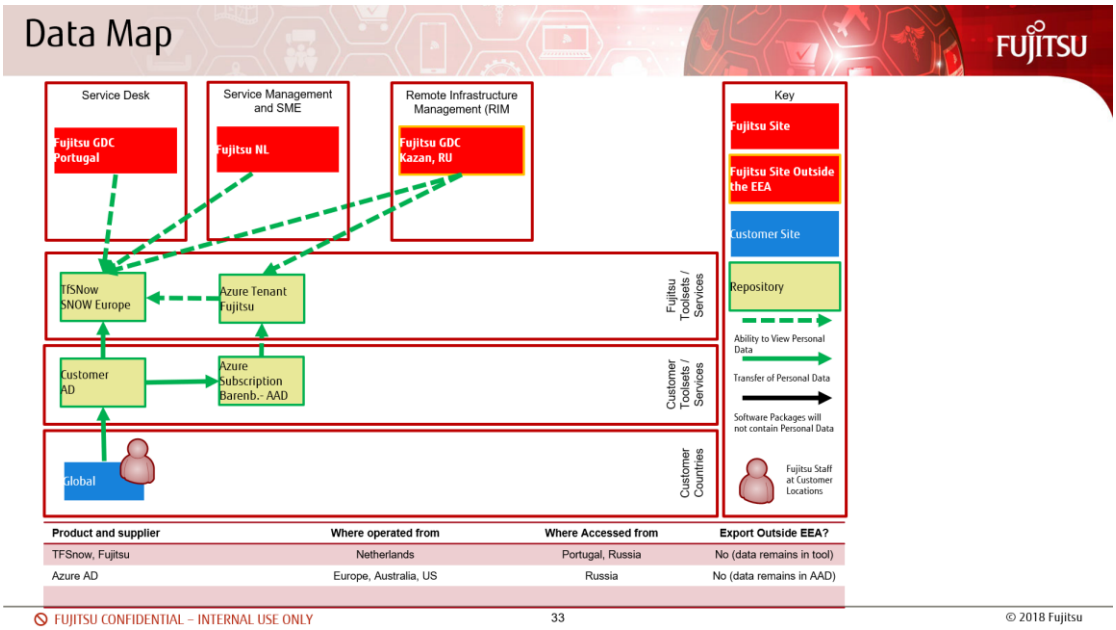
Control	Description and/or Link
Boundary Controls	
Network Device configuration and access	Access to network devices console is authorized via Cisco Meraki dashboard service
Demilitarised Zone (DMZ)	Microsoft Hyper-V servers will be placed into dedicated VLAN. Network access can be restricted per requirements
Internal Network Controls	
Controlled Wireless Access	See details in the LLD sections
Controlled LAN Access	See details in the LLD sections
Encryption Controls	
Wide Area Networks	See details in the LLD sections

6.2 Compliance

Fujitsu are accountable for compliance with specific regulations, dependant on the scope and nature of the proposed solution. Information can be found on local Fujitsu governance sites.

6.3 Data Map

Figure 6 Data Map



Type of Personal Data	Where Held	Where Accessed	Export outside the EEA?

Section B – Infrastructure Design - Low Level

7. Naming and numbering convention

7.1 Location list and naming

TBD

7.2 Device naming

TBD

7.3 IP-addresing

For Barenbrug network private IP-address range of 10.0.0.0/8 is used. This range will be used for all end-user devices, printers, multifunction devices as well as cloud hosted workloads. External IP-addresses for WAN interfaces will be assigned by local ISPs.

Following address ranges will be used:

Region	Site Code	Name	L	M	S	XS	Cloud	Subnet	
Europe	NL01	Barenbrug Holland BV	1					10.32.0.0/16	
Europe	NL02	Barenbrug Wolfheze				1		10.1.0.0/16	
Europe	FR01	Barenbrug France S.A.		1				10.2.0.0/16	
Europe	FR02	Barenbrug Tourneur Recherches				1		10.3.0.0/16	
Europe	FR03	Barenbrug Connantre				1		10.4.0.0/16	
Europe	UK01	Barenbrug UK			1			10.5.0.0/16	
Europe	UK02	Barenbrug UK (Scotland)				1		10.6.0.0/16	
Europe	RO01	Barenbrug Romania				1		10.7.0.0/16	
Europe	BE01	Barenbrug Belgium				1		10.8.0.0/16	
Europe	LU01	Barenbrug Luxemburg S.A.			1			10.9.0.0/16	
Europe	PL01	Barenbrug Polen				1		10.10.0.0/16	
Europe	DK01	Barenbrug Denmark				1		10.11.0.0/16	
Europe	IT01	Barenbrug Italia S.r.l.				1		10.12.0.0/16	
Europe	IT02	Barenbrug Italia (second location)				1		10.33.0.0/16	

Europe	RU01	Barenbrug Russia				1		10.34.0.0/16	
North America	US01	Barenbrug USA (Tangent)		1				10.15.0.0/16	
North America	US02	Barenbrug Albany				1		10.16.0.0/16	
North America	US03	Barenbrug Boardman			1			10.17.0.0/16	
South America	ARG01	Barenbrug Argentina		1				10.18.0.0/16	
South America	BR01	Barenbrug Brazil			1			10.19.0.0/16	
South America	BR02	Barenbrug Brazil		1				10.20.0.0/16	
South America	CL01	Barenbrug Chile				1		10.21.0.0/16	
Oceanic	NZ01	Barenbrug New Zealand		1				10.22.0.0/16	
Oceanic	NZ02	Barenbrug Rolleston				1		10.23.0.0/16	
Oceanic	NZ03	Barenbrug Hamilton (seasonal warehouse)				1		10.24.0.0/16	
Oceanic	AU01	Barenbrug VICTORIA (HEAD OFFICE)		1				10.25.0.0/16	
Oceanic	AU02	Barenbrug SOUTH AUSTRALIA			1			10.26.0.0/16	
Oceanic	AU03	Barenbrug QUEENSLAND				1		10.27.0.0/16	
Oceanic	AU04	Barenbrug HOWLONG				1		10.28.0.0/16	
Oceanic	AU05	Barenbrug TOOWOOMBA				1		10.29.0.0/16	
Oceanic	AU06	Barenbrug WALKAMIN				1		10.30.0.0/16	
Africa	SA01	Barenbrug South Africa			1			10.31.0.0/16	
Cloud EU	WE	Azure EU West					1	10.64.0.0/16	
Cloud US	WU	Azure US West					1	10.65.0.0/16	
Cloud AU	CAU	Azure AU Central					1	10.66.0.0/16	

			1	6	6	19	3		

Following breakdown of IP-address space within site will be used.

Subnet	IP-address range	VLAN#	Description
10.X.101.0/24	10.X.101.4-254/24	101	End users wireless and wired.
10.X.102.0/24	10.X.102.4-254/24	102	End users wireless and wired. Extra space for large sites
10.X.103.0/24	10.X.103.4-254/24	103	Printers and multifunction printing devices
10.X.104.0/24	10.X.104.4-254/24	104	IP-cameras
10.X.105.0/24	10.X.105.4-254/24	105	IP-telephony devices, SSID for wireless VoIP phones
10.X.106.0/24	10.X.106.4-254/24	105	Meeting room devices
10.X.111.0/24	10.X.111.4-254/24	111	Factory machines
10.X.112.0/24	10.X.112.4-254/24	112	Meeting room devices
10.X.199.0/24	10.X.199.4-254/24	199	Guest VLAN, for guest SSID
10.X.201.0/24	10.X.201.4-254/24	201	Management for network and server equipment
10.X.202.0/24	10.X.202.4-254/24	202	Production VLAN for server equipment
10.X.203.0/24	10.X.203.4-254/24	203	Reserved for virtualization services
10.X.254.0/24	10.X.254.1-254/24	-	Service IP range, p2p links, service subnets etc.

First three IP-addresses within each subnet will be reserved for Network equipment and will not be assigned to end hosts (for 10.X.101.0/24 - 10.X.101.1, 10.X.101.2, 10.X.101.3 will be reserved)

Second octet is marked as X as it depends on specific site.

Azure VNET subnets breakdown is provided in Azure Infrastructure design document.

7.4 VLAN-numbering

VLAN numbering will follow general scheme:

- 10x VLANs will be used for end users and devices
- 11x VLANs will be used for manufacturing equipment (scanners, plant floor machinery, warehouse equipment etc.)
- 199 VLAN for guest equipment
- 2xx VLANs will be used for network and server equipment

Further VLAN breakdown within ranges is provided in table below.

VLAN#	Description
101	End users wireless and wired.
102	End users wireless and wired. Extra space for large sites
103	Printers and multifunction printing devices
104	IP-cameras
105	IP-telephony devices, SSID for wireless VoIP phones
105	Meeting room devices
111	Factory machines
112	Meeting room devices
199	Guest VLAN, for guest SSID
201	Management for network and server equipment
202	Production VLAN for server equipment
203	Reserved for virtualization services
211	R&D lab equipment

Azure VNET subnets breakdown is provided in Azure Infrastructure design document.

8. Detailed network configuration

8.1 Cisco MX configuration

8.1.1 General information

Cisco Meraki MX security appliance will be used as aggregation firewall at Barenbrug locations. MX appliance will perform following functions:

- VLAN termination and Inter-VLAN routing
- Setup and maintain WAN and Internet connection
- Setup and maintain VPN tunnel to the hub location
- Network address translation (NAT)
- Traffic filtering

All of these functions are described below in this section.

vMX – virtual Meraki appliance for Azure will be described in Azure Infrastructure design.

8.1.2 VLAN configuration

The MX appliance will be deployed in Routed mode. In this mode, the MX appliance is default gateway for devices on the LAN. Number of VLANs will be configured and terminated on MX appliance according to VLAN numbering and IP-addressing conventions. MX appliance will be routing traffic between local VLANs as well as from local VLANs to Internet or VPN.

SVI-interfaces on Cisco Meraki MX appliance will have 10.X.Y.1/24 IP-address. X and Y are different for each location and VLAN.

8.1.3 WAN and Internet connection

Every Barenbrug office will have Internet connection and It's going to be used as underlay for VPN connection to central hub. VPN traffic will be encrypted and sent over Internet to hub in order to access central services. Return traffic will be also encrypted.

Internet connection parameters like IP-address, default gateway and DNS-server normally will be provided by local ISP and will be configured manually on MX appliance. Once MX appliance is installed and online, it is ready to communicate with the Meraki cloud to download available firmware updates and initial configuration.

Static routing will be used on central and local sites. This decision is dictated by small number of locations and simple routing configuration. Static routes will be used on spoke sites towards hub. Static routes toward each location will be used on hub.

Static default to Internet gateway will be used to provide Internet access on each remote location.

IP-address of WAN-interface of Cisco Meraki MX appliance will be assigned by local ISP.

8.1.4 VPN configuration

In order to setup secure communication between remote locations and central hub Auto VPN feature will be used. Auto VPN simplifies VPN initial configuration and following maintenance.

Split tunnel VPN mode will be used. Split tunnel sends only intranet traffic over the VPN, while all Internet traffic goes directly to its destination. This will optimize traffic routing and offload Internet traffic from VPN connections.

Inner IP-address of IPSec tunnel for every physical location would be 10.X.254.2/24, where X – is location dependent value. Inner IP-addres of IPSec tunnel on cloud side at vMX virtual appliance would be 10.X.254.1/24.

Client VPN server at hub cloud locations will be configured to allow remote clients to connect to corporate network. Client VPN server will be used by "lonely users" and remote workers while traveling or from home locations.

Client VPN server will authenticate remote users via Active Directory server. Cloud active directory server will be used for user authentications.

Client will be able to select closest VPN server based on location.

8.1.5 Routing at central hub

At the hub location static routing will be used to direct traffic to respective VPN tunnel. One static route per physical site will be configured on hub vMX appliance. This will provide traffic reachability from any to any location while keep configuration simple.

8.1.6 Address translation

Client traffic to the Internet will have its source IP rewritten to match the WAN IP of the appliance. Client traffic to Internal addresses via VPN will have its source address unchanged.

Any internal servers publishing to the Internet (DMZ) is not covered in this design.

8.1.7 Traffic filtering

The MX appliance can act as a layer 7 firewall to isolate and protect LAN traffic from the Internet (WAN). It can also filter traffic between LAN and VPN segments. Detailed firewall rules on Cisco Meraki MX appliance is not covered in this document.

8.1.8 DHCP and DNS service

DHCP (Dynamic Host Configuration Protocol) will be configured on every physical aggregation firewall (Cisco Meraki MX physical appliance) in order to provide IP configuration to end users. DHCP service will provide IP-address and mask, default gateway, DNS-servers to wireless and wired end hosts.

DHCP server on MX appliance will be serving requests from local hosts only. If site contains local servers or VMs, they will be configured manually according to IP-address plan.

Meraki MX appliance will be acting as DNS forwarder for local requests (those will be forwarded to AD DNS-server) and for global requests.

8.1.9 Logging and monitoring

To be updated

8.2 Cisco MS configuration

8.2.1 General information

Cisco Meraki MS appliances will be used as access switches at Barenbrug locations. MS switches will perform following functions:

- End hosts connection and uplink connection
- Traffic separation with VLANs

8.2.2 VLAN configuration

Switch uplink interfaces connected to upstream MX appliances will be configured as trunk ports with all VLANs allowed.

Switch ports with end user devices connected will be configured as access ports with respective VLAN configured.

8.2.3 Spanning tree configuration

Rapid Spanning Tree protocol (RSTP) will be configured on all access layer switches.

For switches on small sites it will be using priority of 4096. For medium sites one switch will be using priority of 4096, second will be using default value of 32768.

Since MX appliances connecting access switches does not participate in Spanning Tree protocol and just forwards BPDUs It will be transparent for Spanning Tree topology.

8.3 Cisco MR configuration

8.3.1 General information

Cisco Meraki MR appliances will be used as wireless access pints at Barenbrug locations. MR access points will perform following functions:

- Wireless end hosts connection to the network
- Wireless users authentication

8.3.2 Mode of operation

Wireless Access Points (WAPs) Cisco Meraki MR will be running in bridge mode. In bridge mode, the Meraki APs will act as bridges, allowing wireless clients to obtain their IP addresses from an upstream DHCP server. This mode will allow direct communication between wired and wireless end points within Barenbrug location network.

Meraki APs will be associating wireless clients with end user VLAN per VLAN numbering convention.

8.3.3 Authentication and encryption

Meraki APs will be using pre-shared key (PSK) with WPA2-Personal (Wi-Fi Protected Access) encryption for client authentication. PSK will be deployed to end user hosts automatically and no configuration by users will be required.

8.4 Physical Components Placement

Full list of equipment and its placement will be added here upon design completion.

8.5 Code of Connection

Physical connections at all locations will be unified and fowling common scheme. Uplink and downlink port numbers will be the same at all sites. This will simplify deployment and further operations.

Table below provides connection details.

Description	Definition of Connection	Design and implementation
MX appliance to ISP circuit	Internet1	Interface configuration will be provided by local ISP
MX appliance to access switch #1	Port3	Trunk port
MX appliance to access switch #2	Port4	Trunk port
MS appliance #1 to MR access point #1	Port1	Access port, VLAN

MS appliance #1 to MR access point #2	Port2	Access port, VLAN
MS appliance #1 to MR access point #3	Port3	Access port, VLAN
MS appliance #2 to MR access point #4	Port1	Access port, VLAN
MS appliance #2 to MR access point #5	Eth2	Access port, VLAN

8.6 Bill of Materials

Bill of materials for each type of Barenbrug location is provided below.

Extra Small site BoM:

Part Number	Description	Qty
MX68W-HW	Meraki MX68W Router/Security Appliance	1
LIC-MX68W-SEC-5YR	Meraki MX68W Advanced Security License and Support, 5YR	1
CON-ROBP-MX68WHW	RMA ONLY 8X5XNBDOS-Meraki MXW68 Rou/Sec Appl	1

Small site BoM:

Part Number	Description	Qty
MX68-HW	Meraki MX68 Router/Security Appliance	1
LIC-MX68-SEC-5YR	Meraki MX68 Advanced Security License and Support, 5YR	1
CON-ROBP-MX68HW	RMA ONLY 8X5XNBDOS-Meraki MX68 Rou/Sec Appl	1
MS210-24P-HW	Meraki MS210-24P 1G L2 Cld-Mngd 24x GigE 370W PoE Switch	1
LIC-MS210-24P-5YR	Meraki MS210-24P Enterprise License and Support, 5 Year	1
CON-ROBP-MS210P2W	RMA ONLY 8X5XNBDOS Meraki MS210-24P 1G L2 Cld-Mngd 24x GigE	1
MR42-HW	Meraki MR42 Cloud Managed AP	3
LIC-MR-ADV-5Y	Meraki MR Advanced License and Support, 5YR	3
CON-ROBP-MR42-HW	RMA ONLY 8X5XNBDOS Meraki MR42 Cloud Managed AP	3

Medium site BoM:

Part Number	Description	Qty
MX68-HW	Meraki MX68 Router/Security Appliance	1

LIC-MX68-SEC-5YR	Meraki MX68 Advanced Security License and Support, 5YR	1
CON-ROBP-MX68HW	RMA ONLY 8X5XNBDOS-Meraki MX68 Rou/Sec Appl	1
MS210-24P-HW	Meraki MS210-24P 1G L2 Cld-Mngd 24x GigE 370W PoE Switch	2
LIC-MS210-24P-5YR	Meraki MS210-24P Enterprise License and Support, 5 Year	2
CON-ROBP-MS210P2W	RMA ONLY 8X5XNBDOS Meraki MS210-24P 1G L2 Cld-Mngd 24x GigE	2
MR42-HW	Meraki MR42 Cloud Managed AP	5
LIC-MR-ADV-5Y	Meraki MR Advanced License and Support, 5YR	5
CON-ROBP-MR42-HW	RMA ONLY 8X5XNBDOS Meraki MR42 Cloud Managed AP	5

Section C – Appendices as Required

9. Glossary of Terms

Term/Abbrev	Definition
BoM	Bill of Materials
ISP	Internet Service Provider
LAN	Local Area Network
NAT	Network Address Translation
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WPA	Wi-Fi Protected Access
WAP	Wireless Access Point

10. Document Control

Parameter	Value
Title:	
Component	
Summary:	
Document Author:	
Status:	
Authorisation:	
Next Review Date:	
Distribution:	
Classification:	

11. Change History

This is for the completed ID (Template Governance is elsewhere)

Version control			
VERSION	DATE	CONTRIBUTOR	CHANGE
00.05	19.05.2020	Alexey Protchenkov	First draft
00.07	29.05.2020	Alexey Protchenkov	IP-addressing, PSwitches, multi-hub, RAID
00.09	02.10.2020	Alexey Protchenkov	Updates after Barenbrug review
00.10	05.10.2020	Alexey Protchenkov	Updates after Internal FJ review
1.0	20.01.2021	Stefan van Aarle	Approved

Review control			
VERSION	DATE	REVIEWER	STATUS
[01.00]	20/01/2021	Stefan van Aarle	Approved