Infrastructure Network Design HLD   
Technical Design for Network infrastructure on Barenbrug project

Document details

Version: 1.14

Last Updated: 30.06.2021

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.

Copyright: © Copyright Fujitsu 2021. All rights reserved. Other than for the purpose of evaluation, as set out under "Non-disclosure" above, no part of this document may be reproduced, stored or transmitted in any form without the prior written permission of Fujitsu.

Contents

[Contents 2](#_Toc72332214)

[Section A – Infrastructure Design - High Level 3](#_Toc72332215)

[1. Introduction & Background 3](#_Toc72332216)

[1.1 Scope & Requirements 3](#_Toc72332217)

[2. Risks, Assumptions, Issues, Dependencies and Constraints 4](#_Toc72332218)

[2.1 Risks 4](#_Toc72332219)

[2.2 Assumptions 4](#_Toc72332220)

[2.3 Issues 5](#_Toc72332221)

[2.4 Dependencies 5](#_Toc72332222)

[2.5 Constraints (Standards, Policies, Guidelines) 5](#_Toc72332223)

[3. High Level Design 6](#_Toc72332224)

[3.1 Design Overview & Description 6](#_Toc72332225)

[3.1.1 Global WAN configuration 6](#_Toc72332226)

[3.1.2 LAN physical configuration 6](#_Toc72332227)

[3.1.3 LAN logical configuration 8](#_Toc72332228)

[3.2 Design Decisions 9](#_Toc72332229)

[3.3 Impact on Existing Infrastructures 10](#_Toc72332230)

[3.4 Decommissioning 10](#_Toc72332231)

[3.5 Interoperability & Integrations 10](#_Toc72332232)

[3.6 Test & Validation 10](#_Toc72332233)

[4. Non-Functional Requirements Approach 11](#_Toc72332234)

[4.1 Availability & Resilience 11](#_Toc72332235)

[4.1.1 Backup and Restore 11](#_Toc72332236)

[4.2 Capacity and Performance Management 11](#_Toc72332237)

[4.2.1 Sizing Assumptions 11](#_Toc72332238)

[4.2.2 Customer Data 11](#_Toc72332239)

[4.2.3 Growth and Sizing (Current and Future) 12](#_Toc72332240)

[5. Enterprise Management & Supportability 13](#_Toc72332241)

[5.1 Remote Support 13](#_Toc72332242)

[5.2 Monitoring 13](#_Toc72332243)

[6. Security, Compliance & Data Map 14](#_Toc72332244)

[6.1 Security 14](#_Toc72332245)

[6.2 Compliance 14](#_Toc72332246)

[6.3 Data Map 14](#_Toc72332247)

[Section C – Appendices as Required 15](#_Toc72332248)

[7. References 16](#_Toc72332249)

[8. Glossary of Terms 17](#_Toc72332250)

[9. Document Control 18](#_Toc72332251)

[10. Change History 19](#_Toc72332252)

# Section A – Infrastructure Design - High Level

# 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.

## Scope & Requirements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ref | Requirement | Source | Req Met  (Y/N) | Action taken |
| REQ001 | New green field network design has to be developed for Barenbrug | AoD | Y | Design has been developed |
| REQ002 | Network design will be based on best practice with limited information regarding existing network infrastructure | AoD | Y | Cisco Meraki best practices have been used |
| REQ003 | No migration of existing infrastructure is required in this design | AoD | Y | Migration is in scope of another project |

# Risks, Assumptions, Issues, Dependencies and Constraints

## 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 it fails Azure will be totally not available for customer | Accepted by Barenbrug |  |  |  |
| RISK002 |  | No network redundancy at customer locations. If network gear or Internet circuit is down, no access to cloud hosted services or Internet | Accepted by Barenbrug |  |  |  |

## 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 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 cannot be pushed to network devices. No Internet connection testing and VPN can be performed for Meraki equipment |  |

## 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 |
|  |  |  |
|  |  |  |

## Dependencies

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

## Constraints (Standards, Policies, Guidelines)

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

# High Level Design

## 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.

### Global WAN configuration

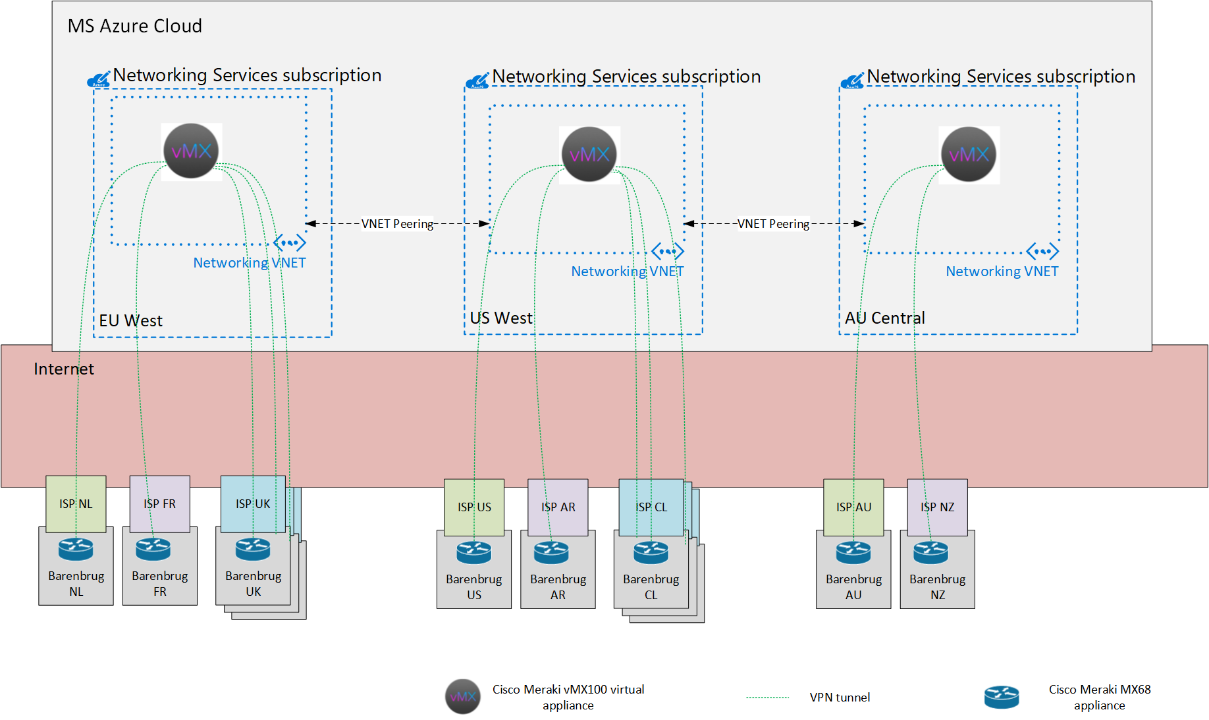
Barenbrug global network topology will follow multi-hub and spokes model. Where hubs will be located at Microsoft Azure public cloud sites with Cisco Meraki virtual appliance deployed as VPN terminating device. Each Barenbrug physical office location will be acting as a spoke and have VPN connection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



### LAN physical configuration

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

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

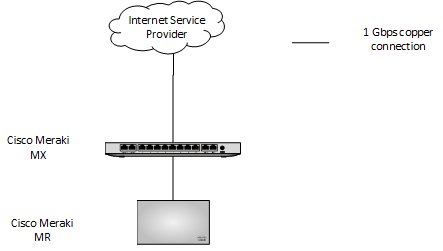
There will be four types of Barenbrug locations depending on number of users at location:

* 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.

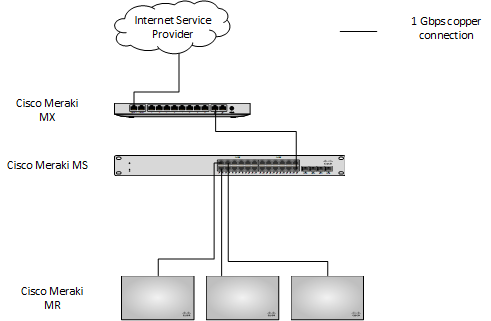
Extra Small site physical diagram is shown below.

Figure 2 Extra Small site network layout



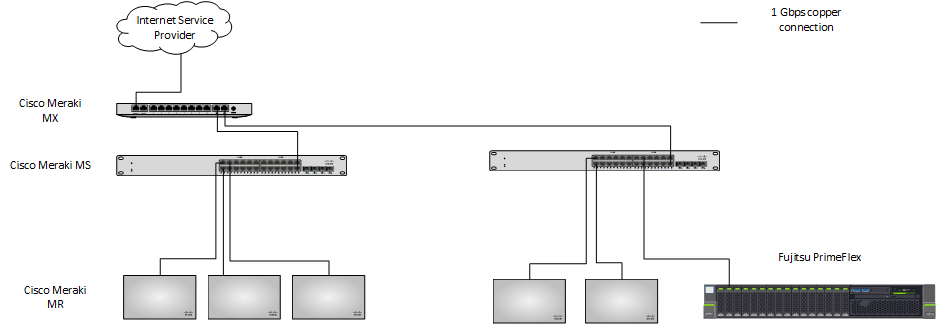
Small site physical diagram is shown below.

Figure 3 Small site network layout



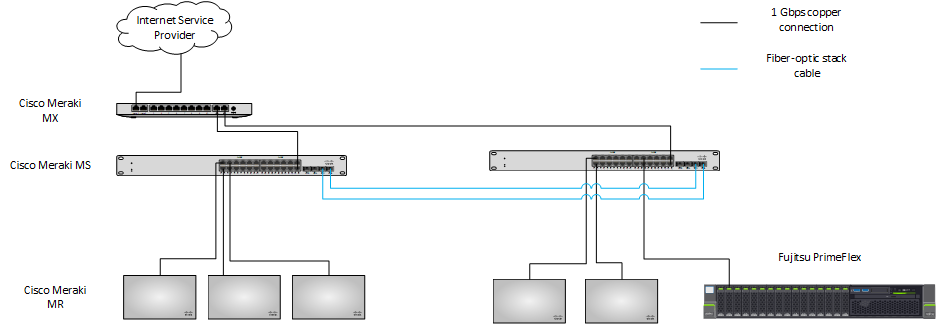
Medium site physical diagrams is shown below.

Figure 4 Medium site network layout (access switches not stacked)



Access switches on Large site and on some medium sites are stacked. Physical diagram for such locations is shown below (Number of access points and servers may vary from site to site).

Figure 5 Network layout for Large site or Medium site with stacked switches



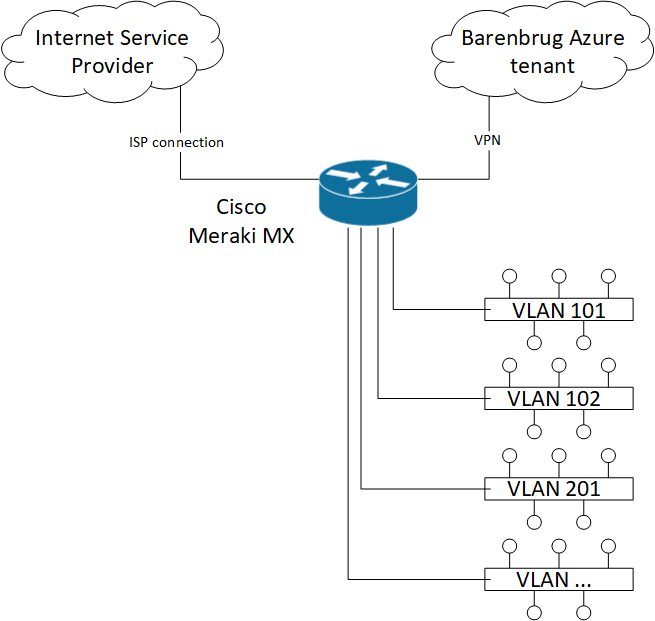
### LAN logical configuration

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 document.

Site logical diagram is shown on picture below.

Figure 5 Branch logical network layout



## 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. |
| MS210 Meraki access switches will be stacked at certain sites | This will simplify management of access switches and will provide some level of redundancy in case of link or switch failure.  List of sites with stacked access switches is provided in LLD document |
| Central AAA server will not be deployed for wireless users authentication | In case of Internet connection failure, wireless users will not be able to reach AAA server and join network, hence local authentication will be used instead. |

## 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.

## Decommissioning

No decommissioning is foreseen as part of this project

## Interoperability & Integrations

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

## 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, VLAN’s, SSID’s. |
| 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 without running any VPN software at end client |

# Non-Functional Requirements Approach

## 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.

### 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.

## Capacity and Performance Management

### 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

### Customer Data

Customer data migration is out of scope of current project.

### 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.

# Enterprise Management & Supportability

## 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.

## Monitoring

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

# Security, Compliance & Data Map

## Security

This document provides the following operational security service components:

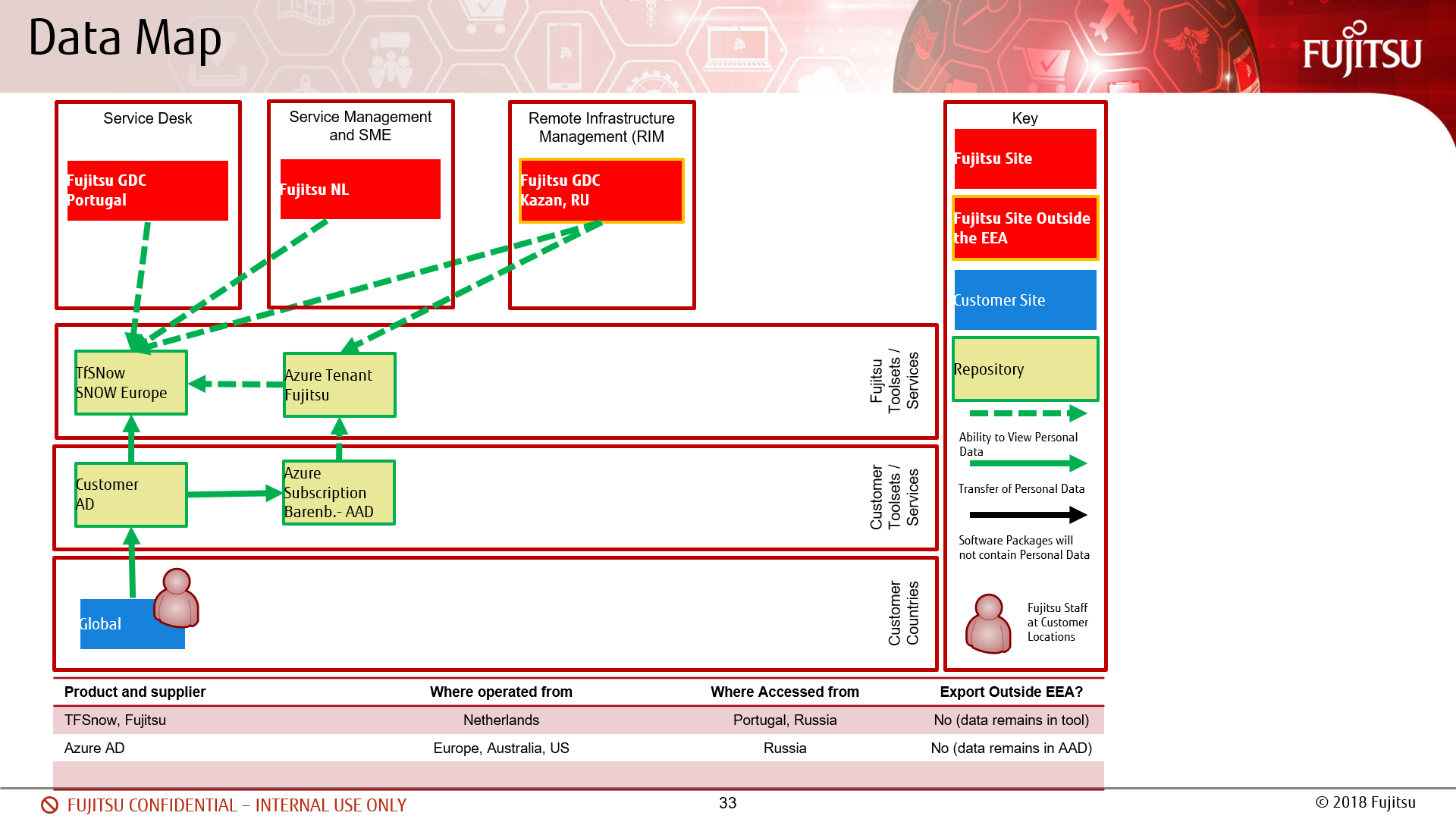
|  |  |
| --- | --- |
| **Control** | **Description and/or Link** |
| **Boundary Controls** |  |
| Network Device configuration and access | Access to network devices console is authorized via Cisco Meraki dashboard service |
| Demilitarised Zone (DMZ) | Microsoft Hyper-V servers will be placed into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

## 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.

## Data Map

Figure 5 Data Map



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

# Section C – Appendices as Required

# References

| **Ref** | **Doc Type** | **Document Reference** | **Description** |
| --- | --- | --- | --- |
|  | HLD/LLD | Azure infrastructure design |  |
|  | HLD/LLD | Hyper-V infrastructure design |  |
|  | HLD/LLD | Network infrastructure design |  |
|  | HLD/LLD | Workplace design |  |
|  | HLD/LLD | Checkmk design |  |
|  | HLD/LLD | App Infrastructure design |  |
|  | LLD | Network LLD |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 |

# Document Control

|  |  |
| --- | --- |
| Parameter | Value |
| Title: | Infrastructure Network Design HLD  Technical Design for Network infrastructure on Barenbrug project |
| Component | Infrastructure |
| Summary: | HLD of Network Infrastructure for Barenbrug |
| Document Author: | Alexey Protchenkov |
| Status: | Release |
| Authorisation: | TBD |
| Next Review Date: | TBD |
| Distribution: |  |
| Classification: | HLD |

# Change History

|  |  |  |  |
| --- | --- | --- | --- |
| 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 | 05.10.2020 | Alexey Protchenkov | Updates after Internal FJ review |
| 1.2 | 17.12.2020 | Alexey Protchenkov | LLD part added |
| 1.3 | 22.12.2020 | Alexey Protchenkov | Used IP-addresses information added |
| 1.4 | 26.01.2021 | Alexey Protchenkov | References to related documents added |
| 1.5 | 01.02.2021 | Alexey Protchenkov | Document cleanup |
| 1.6 | 01.02.2021 | Alexey Protchenkov | vMX config added |
| 1.7 | 01.02.2021 | Alexey Protchenkov | vMX config added |
| 1.8 | 01.02.2021 | Alexey Protchenkov | Cabling details |
| 1.10 | 07.04.2021 | Alexey Protchenkov | Client VPN configuration added |
| 1.11 | 07.05.2021 | Alexey Protchenkov | Document split into HLD and LLD |
| 1.12 | 19.05.2021 | Alexey Protchenkov | Switches stacking on some sites, No Single AAA server decision made. Layout updated |
| 1.13 | 31.05.2021 | Alexey Protchenkov | XSmall site drawing updated |
| 1.14 | 30.06.2021 | Alexey Protchenkov | XSmall site drawing updated |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Review control | | | |
| VERSION | DATE | REVIEWER | STATUS |
| [00.01] | [dd/mm/yyyy] | [Name] | Approved / Remarks |