Location

Standard

Network Security

Responsible Function	IT Infrastructure Team Leader
Organizational Scope	Location Sibiu
Reference (Superior Rule)	Continental Automotive InfoSec & CyberSec Community Wiki > Continental Automotive Information & Cyber Security > Policies, Manuals, Procedures and Methods
Further relevant Rules	-
Key words	Security, Network, Checklist
Functional contact	IT Infrastructure Engineer

Table of Contents

Annexes

-

1 Scope of Content

Objective: This document describes layout, administration and security procedures of main network elements and services.

Goal: Overview of network architecture, security and management process, description of categories and services: design, equipment (active and passive devices), provisioning, implementation and operation according to guidelines and security policies; LAN concepts, devices and services.

Scope: Location Sibiu

2 Network Elements

LAN is designed following the base ideas of *performance*, *security* and *scalability*.

Passive LAN design (copper and optical fiber) follows Continental approved standards for equipment and implementation.

Active LAN design is *3 tier architecture* (core, distribution, access) and is taking into consideration only approved and standard equipment. Components of all network layers are *clustered*.

Design and LAN 3rd Level support is provided by Automotive Network and Voice Team (SLA Standard Support)

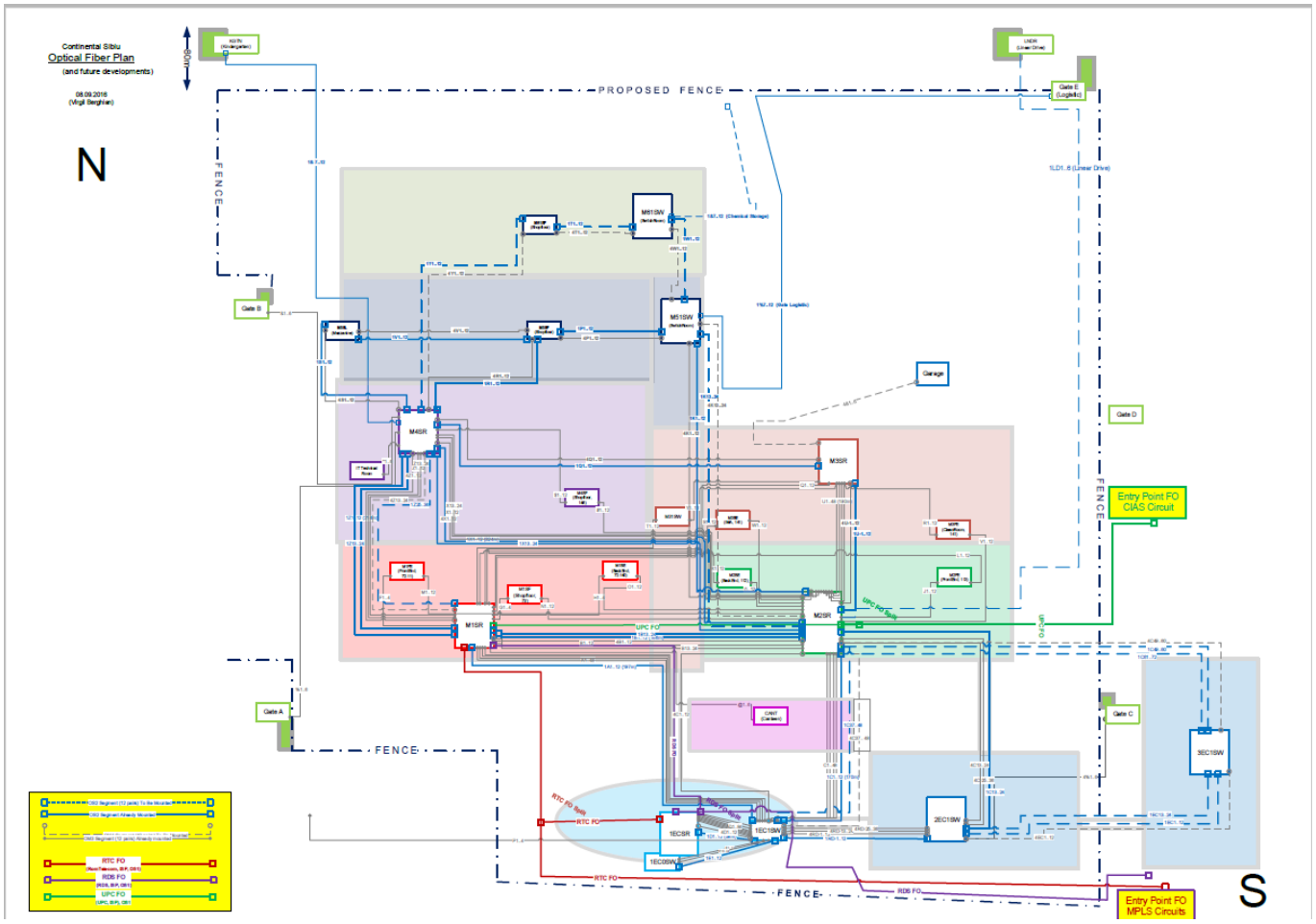
Implementation of passive LAN is usually in responsibility of external supplier, but closely monitored by local IT team to assure compliance with Continental requirements.

Implementation, operation, support and monitor of active LAN devices are the object of local “IT Infrastructure” team’s activity.

2.1 Passive LAN

- ~10K copper ports, around 500 KM copper cable, 40 short-range and 15 long-range optical fiber segments
- Standard Passive Networks manual, Krone and R&M materials, Cat6 certified (Cat7, Real10) measured ports
- LAN extensions as a result of increased workplace density: state the need, request for quotation, supervise and approve works –> IT Infrastructure team
- LAN extension as a result of cabling new building: agreed providers, standard passive components, installed ports measurements, acceptance protocol
- Patching – user support (workplace related activities): local IT Workplace team

Fiber Optic Plan:



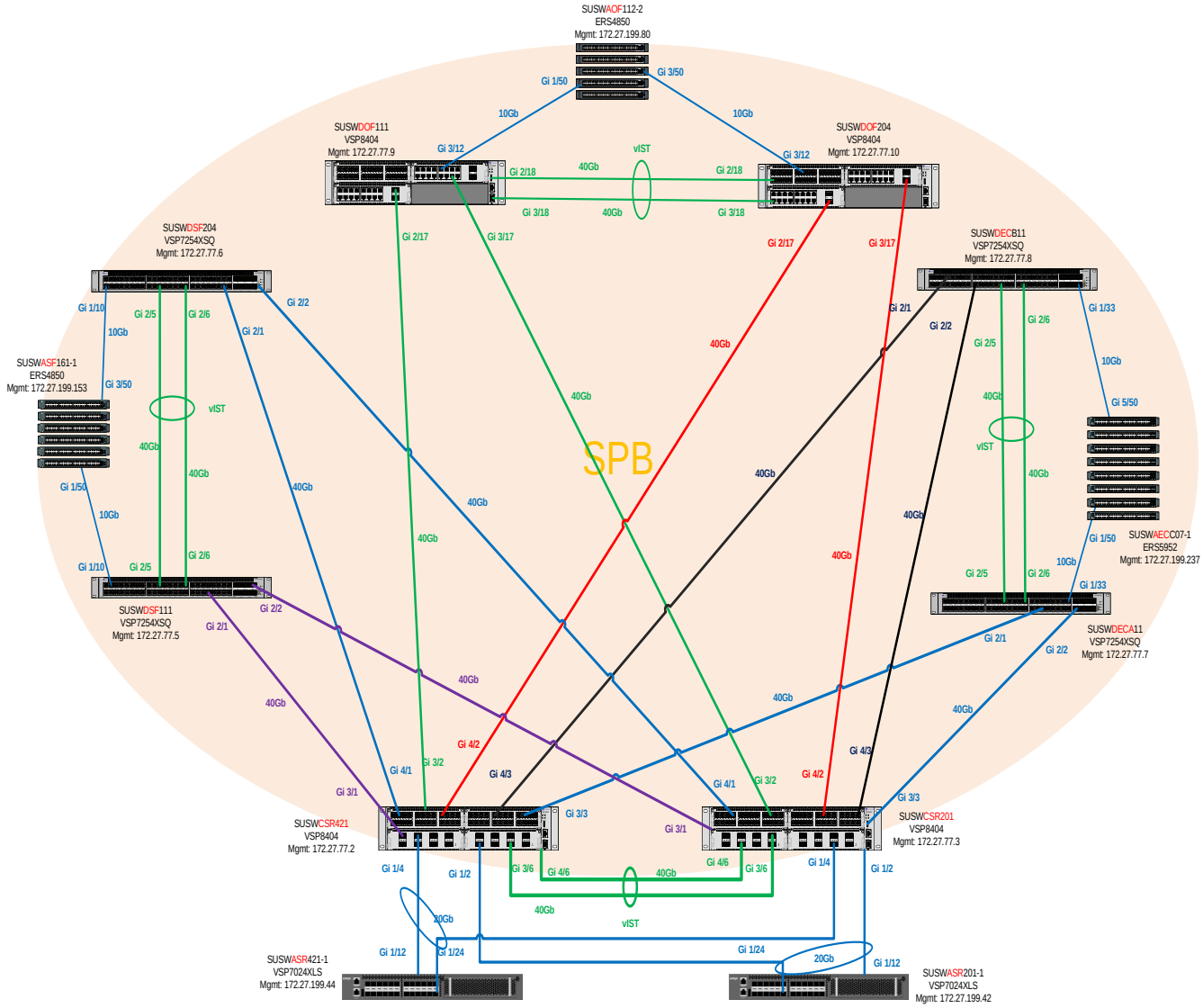
2.2 Active LAN

- design and plans (Level 3 support) are supervised and approved by Automotive Infrastructure Network and Voice team
- clustered active components (Access, Distribution, Core) and redundant paths for connectivity in separate fire zones
- LAN is configured with SPBM (Shortest Path Bridging MAC – 802.1h MAC-in-MAC encapsulation). SPB provides shortest path forwarding using layer 2 to provide shortest path forwarding. SPB uses the IS-IS protocol operating at layer 2 allowing for large networks with fast convergence, equal cost paths and easy provisioning.
- SPBM virtualized services are delineated by I-SIDs.
- Improved security – Client VLAN captive
- ~ 500 managed devices/systems (active LAN components)
- 40G LAN core and distribution, 10G LAN access to clients, 10G LAN access to critical servers, Public network, MIS Storage network

Network Architecture

LAN 3 Tier Architecture (Core, Distribution, Access)

Clients (Shopfloor, Office, R&D) and Servers



Adding new active devices in network:

1. establish the location (rack and position in rack) and the network name of the equipment
2. reserve IP in DHCP server (QIP) in location's correspondent subnet
3. establish cable connection paths, patch-panel's ports, provision and label correct patch-cords and power cables
4. configure spbm instance, configure uplink ports/isis and VLANs/I-SID on the new device and check/config ports (STP, VLAN, I-SID, IP, DHCP RELAY, VRRP) on the Building/Server Core Switch (both IST partners!)
5. configure Security (CLI,SSH, SNMPv3) and Monitoring (syslog, sFlow) on the new device
6. add new device to monitoring systems (NagiosXI, XMC/backup)
7. mount new device in rack and make connections (uplinks, stacking, power)

8. create image / ‘save config’ to the configuration central repository (IT folder structure/Central servers – automatically with XMC – Extreme Management Centers)

9. Add the network equipment in XMC Management tool, Nagios XI (for Monitoring), HPAM (I4.0, for Inventory)

Naming convention

1.Room name - MXSR / XECYSW

Ex. M4SR Module Production number = M4 Room Type = SR (Data Center)

1EC0SW EC number = 1 Module name = EC Floor = 0 Room Type = SW (Distribution Room)

2.Rack name - SURKMXYZ / SURKXECYZ

Ex. SURKM421 SU = Location Sibiu RK = Rack M4 = Module name 2 = Row Number 1 = Nr in Row

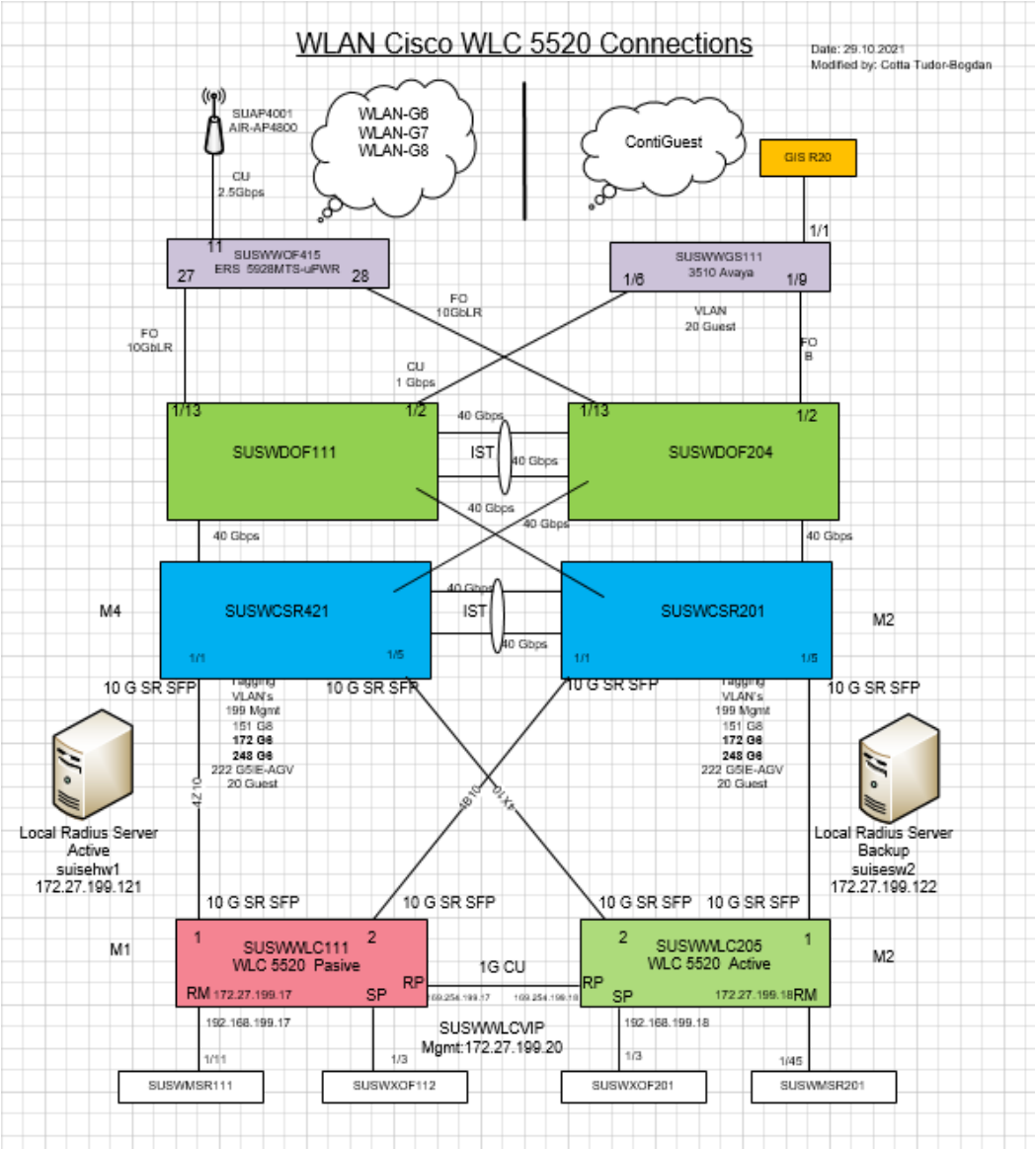
Ex. SURKAEC21 SU = Location Sibiu RK = Rack A = EC Number EC = Engineer Center 2 = Row Number 1 = Nr in Row

3.Switch name - SUSWASFXYZ(B)

Ex. SUSWAOF112-1 SU = Location Sibiu SW = Function (Switch) A = Access Switch(Tier Level) OF = Area which it serves (Office) 1 = Module number 1 = Row Number 2 = Nr in Row 1 = Stack number in rack

2.3 WLAN

- HA SSO Cisco Wireless Controller 5520 (20Gbps uplinks), around 350 APs AIR-AP4800 (PoE) and Catalyst 9130AX(wifi 6)
- authentication 802.1x PEAP - WLAN-G6 / WLAN-G7, centralized authorization – local RADIUS server (2x Cisco ISE), Secure Encryption – WPA2+WPA3/CCPM128(AES)
- authentication WPA/AES-TKIP, WPA2/AES with MAC filtering for WLAN-G8, WLAN-G5IE
- management and monitoring: Configuration and Management with Cisco GUI and Cisco Prime Infrastructure, alerting with NagiosXI



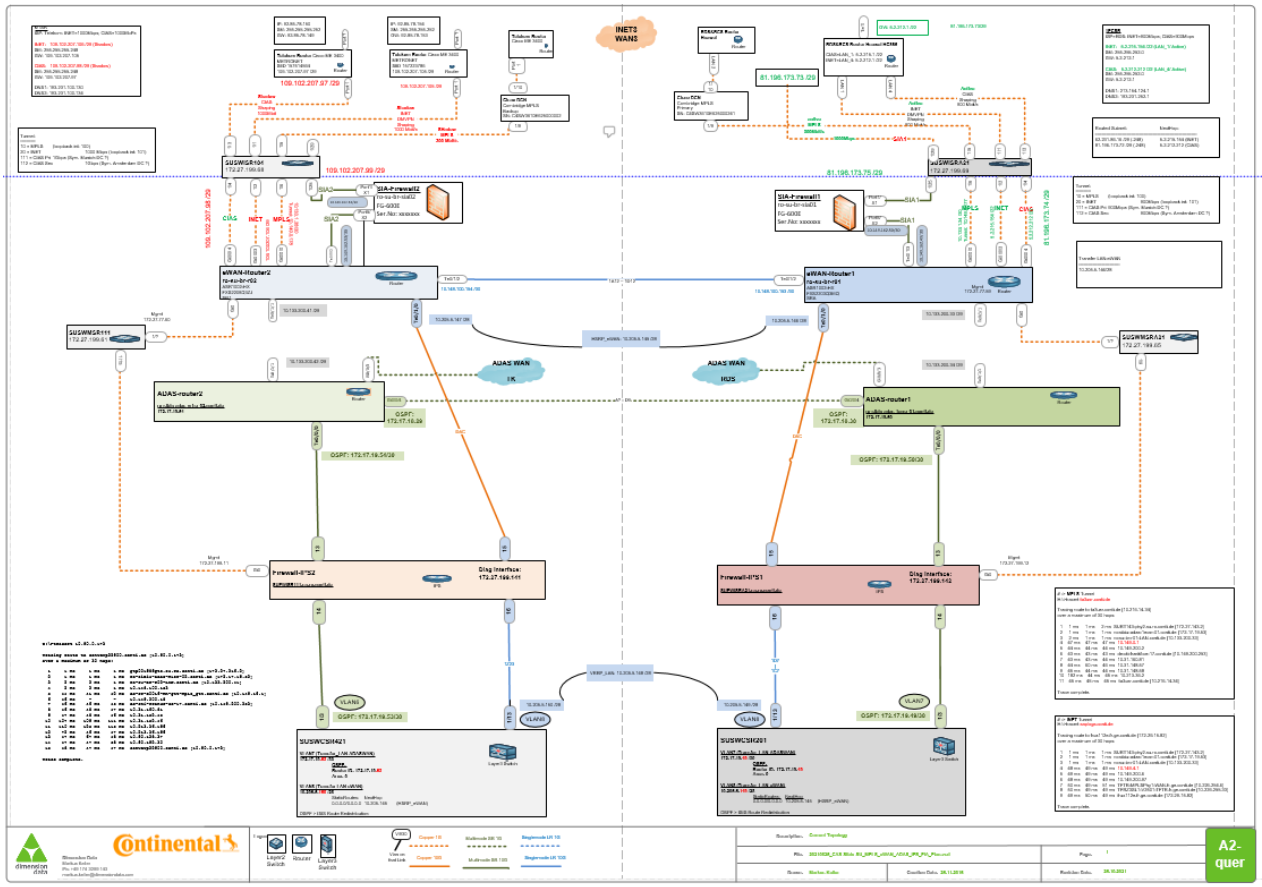
2.4 WAN

2.4.1 eWAN

- 2x eWAN routers – Cisco ASR1002-HX
- 2x MPLS Line, active-passive, 300Mbps
- VPN Tunnels for traffic separation: INET and MPLS
- 2x SIA Line, active-passive, 1000Mbps, 1000Mbps
    - SIA service (local Proxy)
- 2x INET Line, active-passive, 1000Mbps, 1000Mbps
- Intrusion Prevention System in-place

2.4.2 ADAS WAN

- Separate lines for ADAS traffic
- 2x last mile service providers (RDS, Telekom) with 2 separate entry points for HA, Optical Fiber



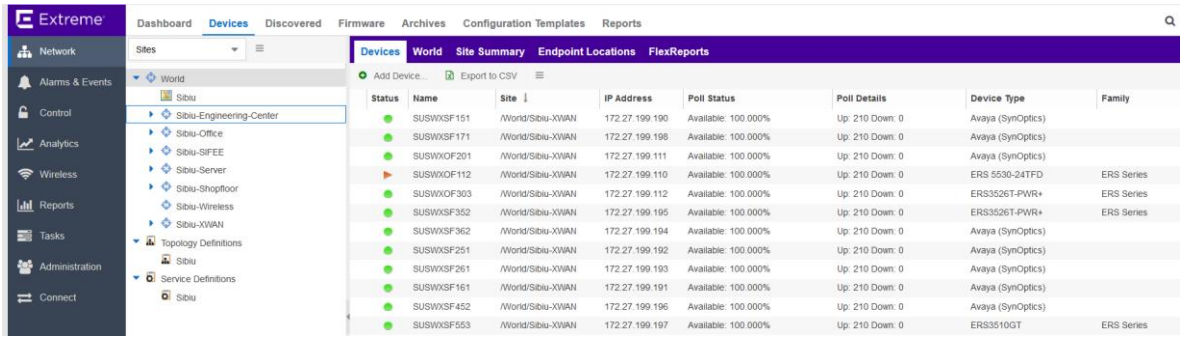
2.5 Telephony

- PBX and VoIP LAN Stacks on Datacenter UPS
- 3CX IP PBX, SIP Trunks

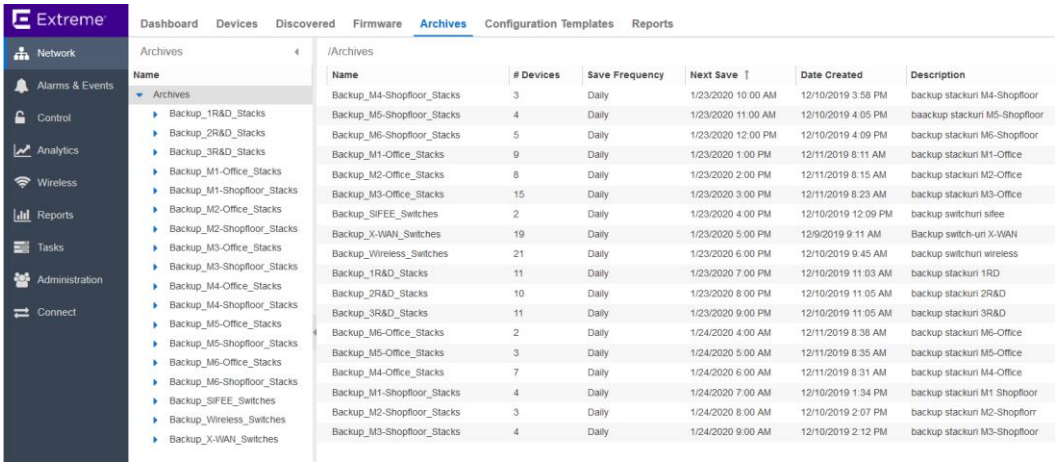
LAN Management and Security

3 LAN Management

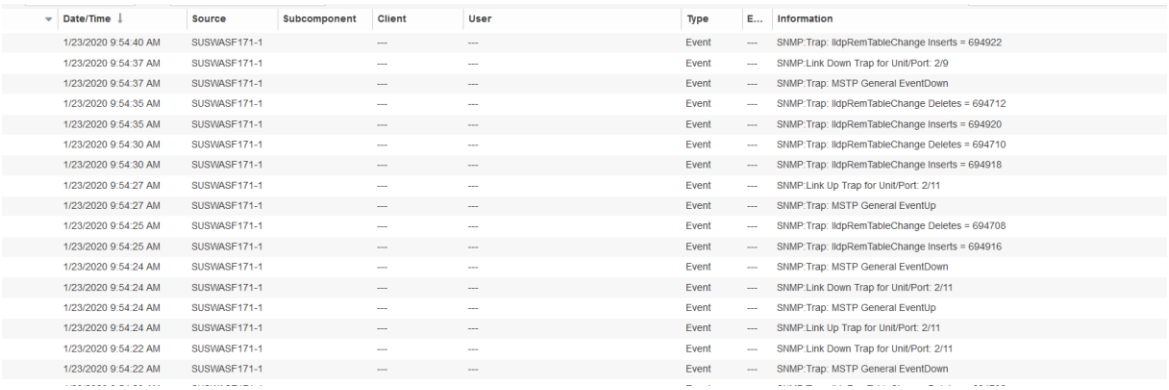
- XMC (Extreme Management Center):
- LDAP Authentication – access only with specific Active Directory Administrative Account
- Role based authentication



Daily Backup for network devices with XMC



Syslog Server – XMC and Corporate Syslog Servers



- Support for planning, sourcing, implementation from central network and voice team
- L3 configuration, troubleshooting, monitoring by local IT with support from central IT
- Support Contract: Avaya Next Business Day - parts replacement for core active components

- **role-based administration**: Network Administrator and Network Operator
- in-band management for Access switch-stacks – CLI and SNMPv3 - RW and RO access

- **out-of-band management** for Core and Distribution switches

Internal

- **Network connection control**
- (CLI, SNMPv3, BPA)
- VPN for Remote Access (Cisco VPN Client)
- Security Patches Process

CLI:

ERS5928, ERS5952, ERS4950, ERS4850, ERS4548, VSP7024, ERS5600

Authorization via TACACS+ : Cisco ISE acts as TACACS Server

Authentication with Active Directory Administrator Account on Access Switches

ERS8404, ERS7254 Special Access

Obed | role read-write

SNMPv3

obed service RW - for Conti Sibiu(XMC)

felix spport RW - for FelixTelecom

saddoc helper RW - for Conti Competence Center

monitor monitor RO - for Conti Sibiu Monitoring

- Extreme Management center: https://suas210-vm:8443
- Cisco Wireless Management System: https://172.27.199.20
- Cisco Prime Infrastructure: https://suas189-vm

4 Security – Network Access Control

Extreme Control tool from Extreme Networks

- 802.1x authentication for capable devices
- MAB (MAC Authentication Bypass) for devices which are not capable for 802.1x
- Automatic VLAN Assignment: Rules, Profiles, Policies
- Access to network is controlled by Extreme Control tool
- Quarantine VLAN

5 Network segmentation

5.1 Subnets and VLANs

Segmentation is implemented as a mapping between class “C” IP subnets and VLANs: every subnet has an associated VLAN and is distributed according topology.

This separation is between office workplaces (where development engineers are sitting) and hosts on production lines.

2 x Segmentation Firewalls – Cisco Firepower 4115Threat Defense

Public network is re-organized in according with new cybersecurity rules.

Two Important categories: Trusted and Untrusted devices and are separated by firewall, untrusted devices are behind firewall and there are configured more than 6500 ACLs.

ACLs are managed with FMC – Firewall Management Center

5.2 Trusted Devices

IP	Subnet	VLAN	VRF					VRF	VLAN	Subnet	IP
					TRUSTED						
					LAN						
					EC		OF				
172.27.80.0/23		1910	0	PCTrust_ECA0_80	Managed PC's		Managed PC's	PCTrust_OF12_120	0	1612	172.27.120.0/23
172.27.184.0/23		1911	0	PCTrust_ECA1_184	Managed PC's						
172.27.160.0/23		1920	0	PCTrust_ECB0_160	Managed PC's		Managed PC's	PCTrust_OF34_124	0	1634	172.27.124.0/23
172.27.164.0/23		1921	0	PCTrust_ECB1_164	Managed PC's						
172.27.228.0/23		1930	0	PCTrust_ECC0_228	Managed PC's		Managed PC's	PCTrust_OF56_216	0	1656	172.27.216.0/23
172.27.232.0/23		1931	0	PCTrust_ECC1_232	Managed PC's						
172.27.240.0/23		1932	0	PCTrust_ECC2_240	Managed PC's						
172.27.244.0/23		1900	0	PCTrust_EC_ADAS_244	Managed PC's ADAS WAN						
172.27.159.0/24		1600	0	VDI_Trust	Managed VDI's			VDI _Trust	0	1600	
					VoIP						
172.27.238.0/23;	238	991	0	VoIP_ECA_238	Option43 String: 01075369656d656e730204000003DF03		Option43 String: 01075369656d656e7302040000	VoIP_OF12_188	0	912	188 172.27.188.0/23;
172.27.192.0/23;	192	992	0	VoIP_ECB_192	01075369656d656e730204000003E003		01075369656d656e7302040000	VoIP_OF34_226	0	934	226 172.27.226.0/23;
172.27.246.0/23	246	993	0	VoIP_ECC_246	Option43 String: 01075369656d656e730204000003E103		Option43 String: 01075369656d656e7302040000	VoIP_OF56_236	0	956	236 172.27.236.0/23;
					WiFi						
					EC		OF, SF				
172.27.248.0/22		248	0	W_PC_Trust_EC	LAPTOP_Trust [WLAN-G6]		LAPTOP_Trust [WLAN-G6]	W_PC_Trust_OF	0	172	172.27.172.0/22
					Servers						
172.27.110.0/24		110	0	SRTrust_110	Sibiu M2-M4-1EC, Cluster, Server						
172.27.150.0/24		150	0	SRTrust_MIS1_150	MIS1 Server						
172.27.190.0/24		190	0	SRTrust_MIS2_190	MIS2 Server						
172.27.191.0/24		191	0	SRTrust_MIS2_191	Data Migration MIS2						
172.27.170.0/24		170	0	SRTrust_CentralMG_170	Centrally Managed Servers						
					Mgmt VLAN (LAN)						
172.27.196.0/23		196	0	AP_MGMT_196	Access Point Management						
172.27.199.0/24		199	0	NW_MGMT_199	LAN Management						
					Transfer VLAN's						
172.30.72.32/28		555	0	CORE_FW	Transfer LAN CORE-FW						
172.17.19.48/28		7	0	ADAS_WAN_7	Transfer LAN-ADAS-WAN						

5.3 Untrusted Devices

IP	Subnet	VLAN	VRF		UNTRUSTED				VRF	VLAN	Subnet	IP
					LAN							
					EC, OF		SF					
172.27.212.0/23	212	600	1	IOT_212	IoT (boardpc, sensors)		IOT (boardpc, cobots, proc_cam, sensors, eKanBan)	IOT_222	1	700	222	172.27.222.0/23
172.27.166.0/23	166	601	1	BMS_166	BMS (Interflex) (FM sensors, access cotrol)							
172.27.186.0/24	186	602	1	BMS_Server_186	SERVER ROOM (APC: UPS, Cooling, Cam, InfrastruXture, Sensors)							
172.27.181.0/24	181	703	0	PRINTER_181	PRINTERS			PRINTER_181	0	703		172.27.181.0/24
172.27.208.0/23	208	711	0	MULTIMEDIA_208	Multimedia (WiPG, TV,Teradici <ZC>)			MULTIMEDIA_208	0	711		172.27.208.0/23
172.27.219.0/24	219	604	1	DEV_DEVICE_219	DEVELOPMENT DEVICES (oscilloscopes, measurement/lab devices)							
172.27.224.0/24	224	609	1	QL_DEVICES_224	Qualification Laboratory (Climatic Chambers, Vibration Control Machines, etc.)							
								PROD_DEVICE_194	3	715	194	172.27.194.0/24
								PROD_DEVICE_720	3	718	720	172.27.72.0/25
		821		AU_SU_FA_Sibiu_R	Sibiu Meeting Room			PROD_DEVICE_195	3	716	195	172.27.195.0/24
		841		AU_SU_FA_TH2_R	Training Hub 2			PROD_DEVICE_721	3	719	721	172.27.72.128/25
								PROD_DEVICE_73	3	717	73	172.27.73.0/24
								PROD_DEVICE_112	3	725	112	172.27.112.0/24
		891		AU_SU_FA_Stk_R_1	Stocken Meeting Room 1 - R&D3 Etaj2			PROD_DEVICE_1110	3	727	1110	172.27.111.0/25
		892		AU_SU_FA_Stk_R_2	Stocken Meeting Room 2 - R&D3 Etaj2			PROD_DEVICE_113	3	726	113	172.27.113.0/24
							PRODUCTION DEVICES Line XX 10.x.x.x/26 (W10, plc, Cox PC*(XP, W7))	PROD_DEVICE_1111	3	728	1111	172.27.111.128/25
								PROD_DEVICE_141	3	736	141	172.27.141.0/24
								PROD_DEVICE_142	3	735	142	172.27.142.0/24
								PROD_DEVICE_221	3	737	221	172.27.221.0/24
								PROD_DEVICE_145	3	745	145	172.27.145.0/24
								PROD_DEVICE_146	3	746	146	172.27.146.0/24
								PROD_DEVICE_76	3	747	76	172.27.76.0/24
								PROD_DEVICE_154	3	755	154	172.27.154.0/23
								PROD_DEVICE_156	3	756	156	172.27.156.0/23
								PROD_DEVICE_115	3	757	115	172.27.115.0/24
								~~PROD_DEVICE_177~~	~~3~~	~~758~~	~~177~~	~~172.27.177.0/24~~
								PROD_DEVICE_210	3	765	210	172.27.210.0/23
~~172.27.214.0/24~~	~~214~~	~~605~~	0	~~PC_UNtrust_ADAS_214~~	~~Unsecure Windows (XP, 7) ADAS_WAN~~		Fazzit	PROD_FAZZIT_171	3	705	171	172.27.171.0/24
172.27.218.0/24	218	606	0	PCUntrust_OF_218	Unsecure Windows (XP, 7) Cox PC's		Fuji NXT	PROD_FUJI_234	3	706	234	172.27.234.0/23
172.27.215.0/24	215	608	0	PCUNtrust_EC_215	Unsecure Windows (XP, 7)							
172.27.180.0/24	180	620	0	PCUntrust_EXT_180	Unsecure PC Extern(KGTN,Gate) - PERIMETER							
172.27.158.0/24	158	613	0	VDI_UNtrust_OF_158	Unsecure Windows (XP, 7) VDI		Unsecure Windows (XP, 7) VDI	VDI_UNtrust_SF_148	0	713	148	172.27.148.0/23
					VoIP							
172.27.238.0/23;	238	991	0	VoIP_ECA_238	01075369656d656e730204000003DF031A73646c703a2f2f3137322e32372e3135302e33373a		01075369656d656e730204000003390031A73646c703a2f2f3137322e32372	VoIP_OF12_188	0	912	188	172.27.188.0/23;
172.27.192.0/23;	192	992	0	VoIP_ECB_192	01075369656d656e730204000003E0031A73646c703a2f2f3137322e32372e3135302e33373a		01075369656d656e730204000003A6031A73646c703a2f2f3137322e32372	VoIP_OF34_226	0	934	226	172.27.226.0/23;
172.27.246.0/23	246	993	0	VoIP_ECC_246	01075369656d656e730204000003E1031A73646c703a2f2f3137322e32372e3135302e33373a		01075369656d656e730204000003BC031A73646c703a2f2f3137322e32372	VoIP_OF56_236	0	956	236	172.27.236.0/23;
					WiFi							
					EC, OF		SF					
172.27.203.0/24	203	707	1	W_IOT	IOT (wearables, boardpc, sensors) [WLAN-G7/G8]			W_IOT	1	707	203	172.27.203.0/24
172.27.187.0/24		607	1	W_PROXY_NoAuth	Device doesn't trigger authentication(meeting bar) [WLAN-G8]			W_PROXY_NoAuth	1	607		172.27.187.0/24
							Scanners [WLAN-G7]	W_SCAN_SF	3	708	151	172.27.151.0/24
							AGV's (Cobots) [WLAN-G7]	W_AGV_SF	3	709	202	172.27.202.0/24
10.138.0.0/23		612	0	W_MOB	Mobile devices (managed by Mobile Iron) [WLAN-G8]			W_MOB	0	612		10.138.0.0/23
10.225.118.0/24		21	0	W_IOT_WAN	IOT (which needs Internet access) [WLAN-G8]			W_IOT_WAN	0	21		10.225.118.0/24
10.225.127.0/24		28	0	W_IGA	IGA (Internet Guest Access) [ContiGuest]			W_IGA	0	28		10.225.127.0/24
					Server							
172.27.220.0/24	220	220	0	SR_Untrust_220	Unpatchable Server(WinSrv2008, Linux old systems)			SR_Untrust_220	0	220	220	172.27.220.0/24
					Mgmt VLAN (Servers)							
172.27.77.0/24	77	77	0	MG_Untrust_77	Server Management (iLO Boards,			MG_Untrust_77	0	77	77	172.27.77.0/24

6 Process performance indicators (KPIs)

Reaction Time (Prio3) - S6_Network_Operations	93.00%
Resolution Time (Prio3) - S6_Network_Operations	93.00%
"Critical Systems Availability LAN (Network CLI Access, Distribution, Core, SRV_Access)"	99.95%
"Critical Systems Availability WAN access (CIAS, iNET, MPLS)"	99.95%
"TC_Traffic_Filtering - Project Performance"	100.00%
"VB_Networks_Access_Control - Project Performance"	100.00%

KPI's are monitored within "IT_TargetMatrix" located in "IT Management Teams" channel.

7 Application

The implementation of the present rule starts with 1st of May 2023.

8 Miscellaneous

8.1 References

8.1.1 Mandatory

Continental Automotive InfoSec & CyberSec Community Wiki > Continental Automotive Information & Cyber Security > Policies, Manuals, Procedures and Methods

Network Security Checklist:

https://intranet.conti.de/resource/blob/1126462/b5b3bef9151f88ef169361d4b8bdaa52/network-security-checklist-data.xlsx

WAN Security Guide (conti.de)

8.2 Definitions and Abbreviations

4 List of Abbreviations

Abbreviation	Description
ACL	Access Control List
AES	Advanced Encryption Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
CoBPAS	Continental Business Partner Access Services
CIAS	Continental Internet Access Service
CSO	Continental Security Officer, Chief Security Officer
DES	Data Encryption Standard
DMZ	Demilitarized Zone
HSRP	Hot Standby Router Protocol
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
LAN	Local Area Network
MPLS	MultiProtocol Label Switching
NIST	National Institute of Standards and Technology
RDC	Regional Distribution Center
RADIUS	Remote Authentication Dial-In User Service
SSH	Secure Shell
SSL	Secure Socket Layer
SNMP	Simple Network Management Protocol
TACACS	Terminal Access Controller Access Control System
VPN	Virtual Private network
VRRP	Virtual Router Redundancy Protocol
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network

9 Approval

eSign: 16046461

Name	Function / Department	Location
George Talpos	Manufacturing Project Leader (Local IT Security Advisor)	Sibiu
Cosmin Sideras	Head of Plant Industrial Engineering. Head of Information Technology. Head of Plant CBS Coaching	Sibiu
Camelia Colceriu	RD QMS Team Leader	Sibiu
Larisa Jecan	Plant QMS Team Leader	Sibiu
Ioana Bujor	RD QMS Specialist	Sibiu
Andreea Unguroiu	Plant QMS Specialist	Sibiu

9.1 Definition and Review Team

The members of the Review Team have reviewed the rule and their feedback has been considered. The Responsible Function keeps records about the review.

Definition Team

Name	Function / Department	Location
Andreea Unguroiu	Plant QMS Specialist	Sibiu

Review Team (Cooperation with affected organizational units)

Name	Function / Department	Location
Virgil Berghian	IT Infrastructure Team Leader	Sibiu

Document History

Version	Responsible Function	Details	Effective
1	IT Infrastructure Team Leader	First edition (former local IT rule)	12/1/2021
2	IT Infrastructure Team Leader	Change the scope	05/01/2023

S-list Id: 16046461
Creation date: 21 Apr 2023 10:24:11
S-list file: CA 1014436-02 SBZ Network Security .pdf
Last action date: 02 May 2023 09:22:53
Status: APPROVED
Duration: 11
Group: QMS Plant Sibiu
Category: Standard Procedure
Sensitive information: Yes
Retention time: 30 years
Explanation: New Scope after SHAPE
Initiator name: Berghian Virgil
Initiator email: virgil.berghian@continental-corporation.com
Initiator department: A AN O SIB IT FIX
Initiator login name: auto\berghianv

Signer	Function	Set type/name	Decision	S-list comments
Talpos George-Alexandru (A AN O SIB IT FIX) auto\uic49029-george-alexandru.talpos@continental-corporation.com	Manufacturing Project Leader	Individual signer	Accept 25 Apr 2023 13:23:06 via eSign	
Sideras Cosmin (A AN O SIB IE FIX) auto\siderasc-cosmin.sideras@continental-corporation.com	Head of Plant Industrial Engineering. Head of Inf	Individual signer	Accept 27 Apr 2023 14:08:37 via eSign	
Colceriu Camelia (A SCT LM SIB SAM VED ESS DE STO P&R&D&VED&PSS NPF) auto\colceriuc-camelia.colceriu@continental-corporation.com	RD QMS Team Leader	Individual signer	Accept 28 Apr 2023 13:44:49 via eSign	
Jecan Larisa-Loredana (A AN O SIB Q) auto\uic08110-larisa-loredana.jecan@continental-corporation.com	Plant QMS Team Leader	Individual signer	Accept 29 Apr 2023 08:04:39 via eSign	
Bujor Ioana (A SCT LM SIB SAM VED ESS DE STO P&R&D&VED&PSS NPF) auto\uia41009-ioana.bujor@continental-corporation.com	RD QMS Specialist	Individual signer	Accept 02 May 2023 09:20:44 via eSign	
Unguroiu Andreea (A AN O SIB Q) auto\uib09542-andreea.unguroiu@continental-corporation.com	Plant QMS Specialist	Individual signer	Accept 02 May 2023 09:22:53 via eSign	