STUTTGART AIRPORT

FSG-Firmenstandard

14 Ausführungsrichtlinie IT Infrastruktur

Autor: Verena Müller

Version: 2023/08

Stand: 04.08.2023

Gültigkeit des Dokuments

Sofern nichts anderes vereinbart wurde, ist das Dokument bis zur Veröffentlichung einer neuen Version im Intranet der FSG gültig, längstens jedoch 15 Monate.

Änderungen

Datum	Letzte Version	Änderung	Kapitel
14.08.2015	2017/01	Erstellung	alle
21.12.2015	2017/01	Absprache mit FI3	
12.05.2017	2017/01	Inhaltliche Prüfung – keine techn. Änderungen	alle
01.08.2019	2017/01	Ergänzung um Netzwerkinfrastruktur	10,12,18,19
26.09.2019	2017/01	Überarbeitung der Kapitel von FB3	7,10,16,17
12.11.2019	2017/01	Einarbeitung Kapitel Adminkonzept (neu 18.5.7) anstatt Adminkonten (alt 18.5.4), Anpassungen	15, 18.5.
13.01.2023	2023/01	Überarbeitung der Themen Telefonie, Netzwerk und Security	19.11, 19.13
13.06.2023	2023/06	Überarbeitung Themen Netzwerk	19.11 und 12.3
04.08.2023	2023/08	Komplettüberarbeitung des Dokuments	

Inhalt

1 Ansprechpartner

Artur Wybranietz
Gruppenleiter
IT Arbeitsplätze und zentrale Systeme

Telefon: +49 711 948-3727
E-Mail: Wybranietz@stuttgart-airport.com

Holger Lindner
Gruppenleiter
Netzinfrastruktur und Security

Telefon: + 49 711 948-2426
E-Mail: Lindner@stuttgart-airport.com

2 Allgemeine Bestimmungen

Grundlagen von Planung, Angebot, Vergabe, Ausführung und Abrechnung sind zusätzlich zu den Vertragsbedingungen die zum Zeitpunkt des Vertragsabschlusses gültigen Ausgaben

- des Gesetzes über technische Arbeitsmittel (Gerätesicherheitsgesetz)
- der Regeln der Sicherheitstechnik und sonstiger am Aufstellungsort geltender Gesetze, Normen und Richtlinien

wie beispielsweise

- der EVB-IT
- der IT-Grundschutz nach BSI
- der VDE - Bestimmungen
- der DIN-Normen bzw. EN-Normen
- der VDI Richtlinien
- der EMV Richtlinien

3 Überblick Systemarchitektur / Systemlandschaft

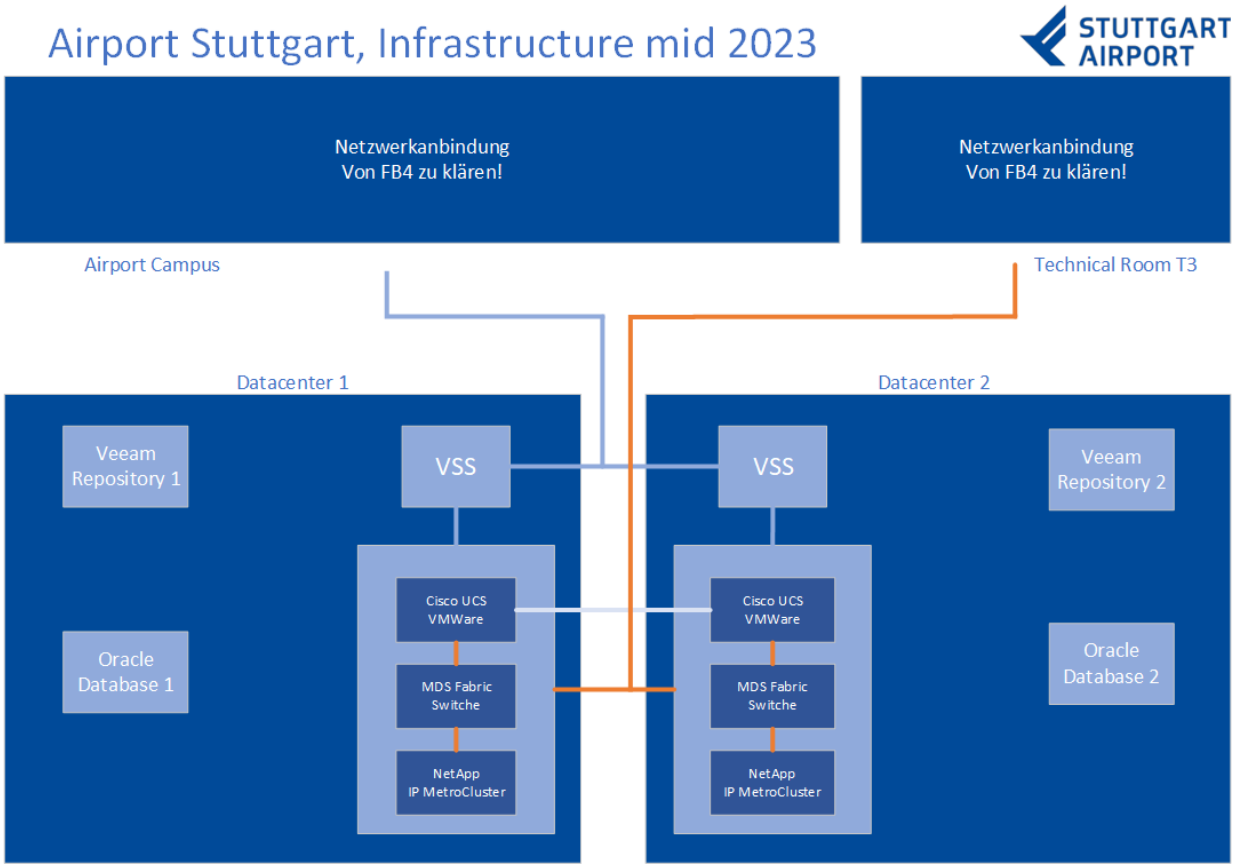

Abbildung 1FSG Infrastruktur

4 Rechenzentren

Die FSG verfügt über zwei Rechenzentren welche mit Klima, USV und Zutrittsschutz (ZKS, EMA und Video) versehen sind.

Der Zutritt zu den Rechenzentren ist nur bestimmten Personen vorbehalten. Diese Personen benötigen eine Einweisung für den Aufenthalt im Rechenzentrum welche durch die RZ-Verantwortlichen nach Absprache durchgeführt wird.

Alle Serversysteme müssen in den Rechenzentren eingestellt werden. Das Aufstellen von Servern außerhalb der Rechenzentren, z.B. in anderen technischen Betriebsräumen, ist nur zulässig sofern eine schriftliche Freigabe durch das IT-Change-Management der FSG vorliegt.

5 Storage

5.1 Allgemein

Das Speichersystem stellt die Speicherbereiche hochverfügbar und ausfallsicher über zwei Rechenzentren zur Verfügung. Die Daten werden synchron und redundant vorgehalten. Im Fehlerfall erfolgt das Umschalten auf den Spiegelbereich Applikationstransparent und ohne Unterbrechung.

Das Speichersystem stellt den eigenen Speicher virtualisiert zur Verfügung.

Alle Speicherbereiche der Storage Lösung sind immer über Kreuz gespiegelt, einzelne nicht gespiegelte Bereiche kommen nicht zum Einsatz.

Eine Unterteilung der Speicherbereiche in Klassen findet nicht statt. Durch die Auswahl und das Design der Laufwerke können die Anforderungen an einen performanten Speicher abgebildet werden.

- Folgende Funktionen werden durch das System bereitgestellt:

Das Speichersystem bietet die Möglichkeit Snapshots zu erstellen.

Erstellen von echten Klonen (sofort replizierte Daten-Volupmes und Datensets) ohne zusätzlichen Storage-Bedarf. Die Erstellung erfolgt ohne Leistungsbeeinflussung.

Die Funktionen Deduplizierung und Komprimierung ist verfügbar.

- Die Systeme sind vollständig in CheckMK (Nagios) integriert.
- Die eingesetzten Host Betriebssysteme werden mittels Multipathing Treiber angebunden.

Für den Betrieb des Gesamtsystems sind zyklisch Updates notwendig. Davon sind auch Komponenten der angebundenen Systeme betroffen (z.B. HBA). Es ist zwingend notwendig, dass auch diese Komponenten bei Bedarf auf die notwendigen Softwarestände angehoben werden. Die Systemverantwortlichen der angeschlossenen Systeme sind verpflichtet diese Updates nach Aufforderung unverzüglich und in Abstimmung mit dem IT-Betrieb einzuspielen.

5.2 Storageeinheiten

Die Storage Controller sind redundant mit jeweils 2xFC pro Fabric angebunden.

Alle Festplatten des Speichersystems sind Hot-Plug fähig.

Durch die Architektur des Speichersystems steht der gesamte Speicherbereich als eine Storage Einheit zur Verfügung.

Die Erweiterung der Nutzkapazität erfolgt ohne Veränderungen für die angebundenen Plattformen.

5.3 Storage Virtualisierung

Das Speichersystem bietet eine Virtualisierung der Speicherbereiche durch den Einsatz von Aggregaten und flexiblen Volumes.

Das Storage System ermöglicht eine logische Darstellung von Daten, die von der physischen Storage-Infrastruktur im Backend unabhängig ist. Dadurch kann direkt auf den Disk Storage im Backend

zurückgegriffen werden, um ein besseres und einheitlicheres Management der virtualisierten Storage Umgebung zu realisieren.

6 Serversysteme

Besteht der Bedarf eines Servers, so sind geeignete Rahmenparameter zu benennen die es dem IT-Betrieb ermöglicht das System zu bemessen und zu entscheiden, ob das System virtuell oder physikalisch bereitgestellt wird. Im Normalfall werden die Systeme virtualisiert zur Verfügung gestellt.

Alle physischen Server sind als Rackversion auszulegen und in den Rechenzentren zu installieren. Diese Server sind in der Regel ohne Maus, Keyboard und Monitor installiert und werden in das zentrale KVM-Konzept der Rechenzentren integriert.

Alle Daten, die ein Server halten soll, sind auf ein SAN-Volume zu schreiben. Die Anbindung des Servers an das SAN erfolgt mittels Fibre-Channel (HBA notwendig).

Alle Server werden mittels eines Systemmanagementsystems überwacht. Dazu sind der Fachabteilung alle Parameter zu nennen die für eine sinnvolle Überwachung des Betriebssystems und der gehosteten Applikationen notwendig sind.

Die Sicherung der Server erfolgt mit Veeam Backup & Replication. Weitere Informationen sind unter 8 Backup/Restore beschrieben.

Standardbetriebssysteme sind Microsoft Server und Linux. Die zu installierenden Versionen und möglichen Derivate sind mit der Fachabteilung festzulegen. Ausnahmen sind zu begründen und über den Changemanager und die Fachabteilung gesondert freizugeben. Die Betriebssysteme müssen zyklisch gepatcht werden. Dazu werden System- und Sicherheitsrelevante Updates monatlich bereitgestellt. Die Definition der Zyklen Bedarf einer Abstimmung mit IT-Security-Manager (FP).. Treiber- oder Applikationsupdates müssen durch die Fachverantwortlichen eingespielt werden, in Abstimmung mit Changemanagement (FP). Der definierte Pachtmanagement Prozess für die jeweilige Lösung / Server ist im Betriebshandbuch festzuhalten.

7 Server Virtualisierung

Wird ein Server virtuell erstellt, werden die Ressourcenzuordnungen nur in begründeten Ausnahmefällen statisch eingetragen. In der Regel werden die Ressourcen dynamisch verwaltet und an den tatsächlichen Bedarf angepasst.

Die Umgebung der FSG ist eine sogenannte virtuelle Infrastruktur, basierend auf den Produkten von VMware vSphere inklusive VMotion, High-Availability (HA) und Distributed Ressource Scheduling (DRS), sowie dem VMware vCenter Server für die zentrale Verwaltung der gesamten Umgebung.

Es gibt drei Datacenter (FSGINT, DMZ und FSGTEST) um die Systeme entsprechend den Sicherheitsanforderungen zu trennen.

Als solides Fundament für die gesamte Umgebung baut das gesamte Konzept auf dem zentralen Storage der FSG auf, um alle benötigten, zentralen Speicherressourcen hochverfügbar gestalten zu können.

Die gesamte virtuelle Infrastruktur für die FSG ist so ausgestattet, dass im Falle eines Ausfalls einer kompletten Seite die verbleibende Infrastruktur die komplette Last tragen kann und die Dienste weiterhin zur Verfügung stehen.

Die Speicherinhalte werden redundant auf den beiden vorhandenen Speichersystemen der FSG abgelegt, wobei die Spiegelung der Daten nicht über den Storage erfolgt, sondern über ein Hostlevelmirroring der virtuellen Umgebung selbst.

Die Datensicherung der virtuellen Maschinen wird durch den Einsatz von Veeam realisiert, um hier eine größtmögliche Zuverlässigkeit und Flexibilität zu bieten.

8 Backup/Restore

Die Datensicherung von virtuellen und physischen Servern bei der Flughafen Stuttgart GmbH erfolgt ausschließlich mit Veeam Backup & Replication. Es bietet Techniken, um Datensicherungen, Wiederherstellungen und Replikationen zu ermöglichen/durchzuführen.

Die Sicherung der Server erfolgt image-basiert (konsistente Sicherung). Das heißt es wird ein komplettes Abbild einer Festplatte, eines Servers oder einer virtuellen Maschine erstellt.

Die Sicherungen erfolgen außerhalb der Servicezeiten (von 18:30 Uhr bis 05:00 Uhr morgens). Im Brandabschnitt 1 werden 14 Restore Points vorgehalten. Im 2. Brandabschnitt liegt eine Kopie der Restore Points und zusätzlich 4x wöchentliche und 6x monatliche Backups.

Sollten andere Anforderungen erwünscht sein, erfolgt dies nur auf Antrag. Damit ist ein Datensicherungskonzept vorzulegen aus dem hervorgeht was gesichert werden soll, in welchem Zyklus und wie wiederhergestellt werden muss (RTO/RPO beachten).

Die Vorgehensweise bei der Datensicherung ist nur auf Sichern und Zurückspielen in einem Fehlerfall ausgelegt. Mit diesen Verfahren werden keine Daten archiviert!

Im Fall einer (Daten-)Wiederherstellung ist das ServiceCenter zu informieren.

9 Corporate Remote Access

Der Teleservice ermöglicht den internen Mitarbeitern der FSG sowie Dritten (externe Wartungsfirmen) über eine VPN-Sitzung ein System Remote zu Warten. Es steht pro System immer nur ein Zugang zur Verfügung, da davon ausgegangen wird, dass immer nur eine Person aus Wartungsgründen zugreift.

Voraussetzung zur Genehmigung eines Remotezuganges

- Das externe Wartungsunternehmen muss gemäß §5 Bundesdatenschutzgesetz eine Verpflichtungserklärung zum Datenschutz unterschreiben.
- Es muss ein Wartungsvertrag bestehen, welcher einen Remote-Zugang vertraglich fixiert, oder die Notwendigkeit aufgrund eines Auftrags (z.B. Projekt oder Maßnahme) vorliegen
- Die Wartungsfirma hat die Personen namentlich zu benennen welche Fernwartungen an dem System durchführen sollen.
- Ein Request for Change (RfC), die unterschriebene Verpflichtungserklärung sowie der Wartungsvertrag ist dem Changemanagement vorzulegen. Das Changemanagement muss der Einrichtung zustimmen.

Vorgehen

Das Wartungsunternehmen erhält einen VPN Remote-Zugang welcher mittels der Lösung Cisco AnyConnect hergestellt wird. Die Authntifizierung bedarf dabei zwei Faktoren; Benutzername und Passwort und Pin/Code Verifizierung durch Microsoft MFA.

Jeder Wartungszugriff muss beim IT-Supportcenter (Tel: 0711-948-3000 07:00 – 16:30 Uhr) oder bei der Leitstelle Technik (Tel: 0711-948-2066 16:30 – 07:00 Uhr) an- und abgemeldet werden. Bei einer geplanten Wartung muss das IT-Supportcenter im Voraus verständigt werden. Die Zugriffe werden durch den Authentisierungsserver der FSG protokolliert.

10 Remoteadministration

10.1 Zugriff auf Serversysteme generell

Der Zugriff auf die Serversysteme ist durch die Dienstanweisung D63 Anlage J Punkt 11 generell geregelt. In den nachfolgenden Absätzen sind die Zugriffsarten auf Serversysteme beschrieben.

Generell gilt, dass für jeden Zugriff auf die Serversysteme ein AD administratives Benutzerkonto notwendig ist. Dies gilt sowohl für die internen wie auch für die externen Benutzer. Die Zugriffe werden durch eine Mitgliedschaft in AD Gruppen beschränkt. Die Gruppen werden pro Server erstellet. Dabei wird nicht zwischen physischen oder virtuellen Systemen unterschieden.

Der RDP-Zugriff auf die Servesysteme ist somit auf die entsprechenden AD Gruppen limitiert.

10.2 Zugriff auf physisch Serversysteme

Für die Remote-Wartung an physischen Serversystemen steht neben dem RDP Zugang eine Webbasierte KVM-Lösung zur Verfügung. Für die Nutzung dieser Lösung wir das entsprechende AD administratives Benutzerkonto für den Zugriff auf die notwendigen Systeme berechtigt.

10.3 Zugriff auf virtuelle Serversysteme unter VMware

Für die Remote-Wartung an virtualisierten Serversystemen steht neben dem RDP Zugang ein VMware Webclient zur Verfügung. Dabei wird über einen Browser eine HTTPS Sitzung aufgebaut. Die dafür notwendigen Berechtigungen werden, dem entsprechenden AD administrativen Benutzerkonto in der VMware Umgebung erteilt.

10.4 Temporäre Support Zugriffe

Ein temporärer Fernzugriff für die Unterstützung der Benutzer durch einen Herstellersupport ist ebenfalls in der Dienstanweisung D63 Anlage J Punkt 11 geregelt. Dieser Zugriff kann über ein Fernsupport Tool z.B TeamViewer geschehen. Dabei ist aber die persönliche Überwachung der Wartungsaktivitäten am Bildschirm Voraussetzung.

10.5 Besondere Zugriffe

Sollen anderweitige Zugriffsarten aus organisatorischen oder technischen Gründen notwendig sein, so sind diese vorab durch das IT-Security-Board und das IT-Change-Management freizugeben und zu dokumentieren.

10.6 Zugriff auf die Clientsysteme

Der Zugriff auf die Clientsysteme darf nur über die SCCM Remoteunterstützung stattfinden. Dabei ist eine Zustimmung des Zugriffs auf den Client durch den Benutzer notwendig. Die Möglichkeit des Zugriffs über SCCM Remoteunterstützung wird durch entsprechende SCCM-Berechtigungsrollen definiert.

10.7 Zugriff auf die Netzwerkinfrastruktur

Für den Zugriff auf die Netzwerkinfrastruktur durch den externen Dienstleister steht eine Cisco VPN Infrastruktur zur Verfügung.

Der Servicedienstleister wählt sich über einen VPN Client (Anyconnect von Cisco) ein und authentifiziert sich mit einem persönlichen Nutzernamen und Passwort. Danach wir eine Authentifizierung mittels zweiten Faktor verlangt, welches derzeit mit Azure MFA als Provider umgesetzt ist.

11 System Monitoring

11.1 Allgemein

Das Monitoring vernetzter Systeme umfasst alle Maßnahmen, die einen effektiven und effizienten, an den Zielen des Unternehmens ausgerichteten Betrieb der Systeme und ihrer Ressourcen sicherstellen. Es dient dazu, die Dienste und Anwendungen der vernetzten Systeme in der gewünschten Güte bereitzustellen und ihre Verfügbarkeit zu gewährleisten. Das System Monitoring dient der Erreichung der nachfolgenden Ziele:

- Es unterstützt die IT-Verantwortlichen wesentlich bei der Bereitstellung von qualifiziertem Support und individuelle Anwenderbetreuung.
- Durch Kontrolle über die einzelnen IT-Systeme sind potenzielle Brennpunkte gezielt zu entschärfen, noch bevor ein größerer Schaden entsteht.
- Es gestattet eine wirkliche Anwenderbetreuung. Durch die Implementierung weitreichender systemtechnischer Informationssysteme können die IT- Mitarbeiter aktiv Kapazitäten freistellen, um dem Anwender im Problemfall, eine schnelle und gezielte Unterstützung zukommen zu lassen.
- Es unterstützt die Beherrschung der eingesetzten IT-Technologien, indem ein effektiver Zugriff auf Systeminformationen von zentraler Stelle aus gegeben ist.
- Es hilft, die Ausfallzeiten zu minimieren. Durch die Überwachung der Systeme sind bei sich abzeichnenden Störungen gezielte Gegenmaßnahmen einzuleiten. Die Reaktionszeit auf ein Problem und die nachfolgende Analyse wird dadurch deutlich verkürzt.

Das System Monitoring behandelt folgende Schwerpunkte:

- Monitoring von Servern und Applikationen
- Monitoring von Netzwerkkomponenten
- Clustern von Ereignissen in einer zentralen Ereigniskonsole
- Graphischer Business View
- Reporting

Als zentrales Monitoring System wird Nagios in Verbindung mit dem Add-On Check_MK eingesetzt. Check_MK ist ein Agenten basierer Aufsatz auf Nagios für die Anbindung von passiven Systemen. Aktive Systeme senden ihre SNMP Traps direkt an das System.

11.2 Servermonitoring

Für die umfassende Überwachung durch Nagios ist ein Maximum von Eventquellen nutzbar zu machen. Es müssen Events aus IT-Systemen, Applikationen, Netzwerkkomponenten, NON- IT-Systemen, usw. in die Überwachung einzubeziehen sein.

Dazu wird die FSG ein Basismonitoring einrichten welches die grundlegenden Werte des Servers überwacht.

Um eine sinnvolle gesamt Überwachung des Zielsystems zu gewährleisten, ist es nötig die darauf gehosteten Dienste bzw. Programme mit entsprechenden Grenzwerten in das Monitoring

aufzunehmen. Dazu werden vom Errichter des Systems die entsprechenden Parameter mit den Grenzwerten geliefert, die zur Erreichung der o.g. Ziele notwendig sind.

11.3 Network Devices

11.3.1 Switche, Router und Access Points

Für die umfassende Überwachung durch Nagios ist ein Maximum von Eventquellen nutzbar zu machen. Es müssen Events aus Switche, Routern, Access Points, Firewall, LAN-/WAN- Verbindungen usw. in die Überwachung einzubeziehen sein.

Die Überwachung der Switche sowie Routern wird mittels SNMP Abfrage umgesetzt:

Folgende Parameter sollen grundsätzlich überwacht werden:

- Systemstatus (online/offline)
- Status von Redundanzen
- Status von Ports (nur ausgewählte Devices)
- Traffic
- Status von Modulen, Lüftern, Netzteilen

Um die o.g. Ziele zu erreichen, werden vom Errichter des Systems die entsprechenden Parameter mit den Grenzwerten geliefert, die zur Erreichung notwendig sind.

11.3.2 USV Systeme

USV Systeme sollen wie folgt überwacht werden:

- Ping
- Systemstatus (online/offline)
- Temperatur
- Zustand des Akkus (Kapazität)

11.3.3 Network Services

Alle IP basierten Services wie http, HTTPS, SMTP, DNS, FTP, POP3, LDAP, NTP, NNTP, Telnet, RADIUS, DHCP können mit folgenden Parametern abgefragt werden:

- Prüfen der Verfügbarkeit
- Prüfen der dienstspezifischen TCP-/UDP- Ports

11.3.4 LAN - / WAN Verbindungen

Bei den Verbindungen sollten folgende Parameter überwacht werden:

- Überprüfung der Verfügbarkeit (steht die Verbindung?)
- Trafficanalyse
- Bandbreitenmessung (bei WAN Verbindungen)

11.4 Event Kategorien

Nagios ist das zentrale Anzeigeinstrument für alle Ereignisse innerhalb der von Nagios überwachten IT- Umgebung und weiterer wichtiger FSG- Systeme (z.B. Alarmrufanlage).

Für die zentrale Ereigniskonsole müssen Events mit unterschiedlicher Wichtigkeit festgelegt werden. Diese Unterscheidung dient der Klassifizierung der eintreffenden Events und stellt ein Kriterium bei der Behandlung dar. Es werden 4 Stufen unterschieden:

- **CRITICAL:** Das Ereignis betrifft zentrale Komponenten und kann Einfluss auf zentrale Prozesse haben. Diese Meldungen können bei Bedarf an den Bereitschafsdienst weitergeleitet werden.
- **WARNING:** Das Ereignis stellt keinen aktuellen akuten Fehlerzustand dar. Es ist vielmehr ein Hinweis zu einer Zustandsänderung, welche auf Alarm gesetzt wurde. Jedoch kann bei Nichtbeachtung ein größerer Fehler entstehen und das Ereignis zu einem CRITICAL werden lassen.
- **OK:** Es gibt kein Ereignis. Das System ist voll verfügbar.

Der Errichter des Systems legt die Stufen mit der FSG für die von ihm definierten Parameter fest.

12 Softwarewartung

Der Begriff bezeichnet „die Veränderung eines Softwareprodukts nach dessen Auslieferung, um Fehler zu beheben, Performanz oder andere Attribute zu verbessern oder Anpassungen an die veränderte Umgebung vorzunehmen.“ (Definition gemäß IEEE 610.12-1990)

Im weiteren Sinne gehören auch Dienstleistungen und Maßnahmen, die die von der Norm beschriebenen Veränderungen begleiten oder unterstützen, zur Softwarewartung. Die Softwarewartung dient in der Regel dazu, die Verwendbarkeit und Betriebssicherheit von Software zu erhalten.

Die FSG setzt dabei in erster Linie auf die präventive Wartung, wobei unter präventiver Wartung die Behebung von solchen Fehlern verstanden wird, die bekannt, aber beim Anwender noch nicht in Erscheinung getreten sind (vgl. IEEE 610.12-1990). Erst bei auftretenden Fehlern wird auf die korrektive Wartung zurückgegriffen.

Grundsätzlich unterliegen alle Systeme der FSG der Softwarewartung. In der Vorgehensweise wird zwischen Clientsystemen und Serversystem unterschieden.

12.1 Clientssysteme

Werden nach einer Testphase mit einem ausgewählten Teilnehmerkreis gemeinsam mit Updates versehen. Upgedatet werden das Betriebssystem und Applikationen, die über das Desktopmanagementsystem gepatcht werden können.

12.2 Serversysteme

Das Ausbringen von Updates auf Server erfolgt individuell und in Absprache mit den Systemverantwortlichen. Ausgebracht wird über den Microsoft WSUS da hierfür keine weiteren Installationen notwendig sind. Die notwendigen Konfigurationsparameter erhalten die Server über entsprechende Gruppenrichtlinien.

Die Aktualisierung der Server bedarf eines vorher definierten Prozesses. Dieser sieht wie folgt aus:

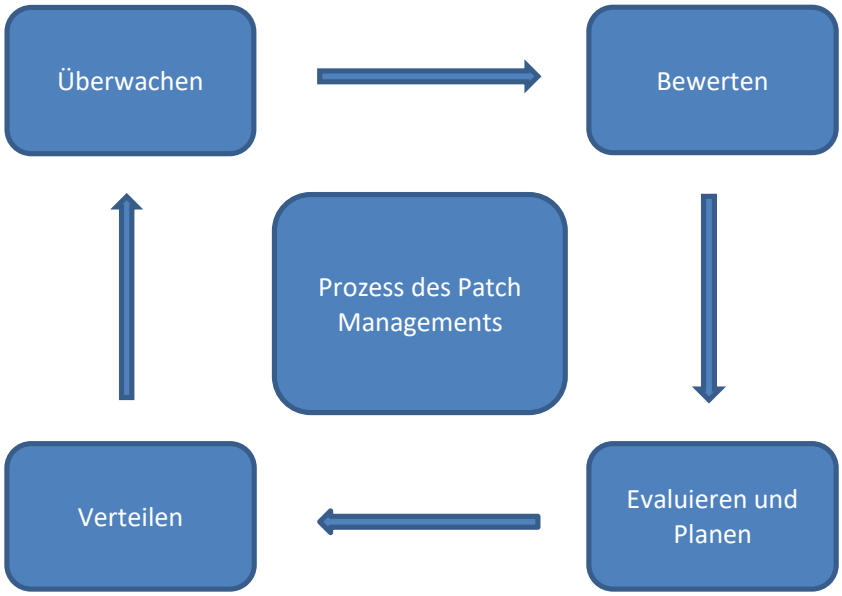

Abbildung 2Softwarewartung Prozess

12.3 Netzwerkkomponenten

Sämtliche Komponenten der Netzwerkinfrastruktur sind in einem AKN Servicevertrag hinsichtlich der Softwarewartung integriert.

Das Ausbringen von Updates auf den Komponenten wie z.B. Switchen erfolgt individuell in enger Absprache mit den Systemverantwortlichen und dem Servicedienstleister.

Die Updates werden über die Cisco Prime Infrastructure an die Switch Komponenten ausgebracht. Teilweise erfolgt die Aktualisierung auch durch manuelles Einspielen der Updates in die entsprechenden Systeme bzw. Komponenten. Dies trifft z.B. auf Managementsysteme / Appliances zu.

13 Mailsystem

Der Flughafen Stuttgart betreibt eine Kommunikationsplattform auf Basis einer Microsoft Exchange Hybrid Umgebung.

Das Mailsystem ist Hochverfügbar und Ausfallsicher installiert. Die Ausfallsicherheit der Hardware ist durch das Virtualisieren der Server gewährleistet. Die notwendigen Exchange Server beinhalten alle Rollen. Eine DAG wurde erstellt, um die Datenbanken Hochverfügbar vorzuhalten. Für die Hochverfügbarkeit der Rollen wurden zwei Loadbalancer eingerichtet. Die Postfächer befinden sich in der Microsoft-Cloud in Deutschland – Exchange Hybrid.

Der Remote Zugriff von außen für Outlook Web App erfolgt über Microsoft direkt per HTTPS. Mit der Hybridstellung können keine Protokolle POP3 und IMAP mehr zur Verfügung gestellt werden. Das Mailsystem der FSG stellt keine „öffentlichen Ordner“ zur Verfügung.

Das Mailsystem kann als Relay für lokale Server verwendet werden. Der Mailverkehr wird wie oben beschrieben über den Loadbalancer geleitet.

Eine revisionssichere Archivierung findet derzeit nicht statt. Exchange Archiv Postfächer (InSitu Archive) werden auftragsbezogen angelegt.

14 Datenbanksysteme

MS-SQL

Bei der FSG kommt als Standarddatenbanksystem Microsoft SQL zum Einsatz.

Datenbanken können auf zwei unterschiedlich Weisen zur Verfügung gestellt werden:

- Sie können als eigenständiger Server konzipiert werden. Dazu sind aber ausführliche Begründungen beizulegen, welche die Notwendigkeit erläutern inkl. einer Risikobewertung.
- Sie werden auf einem bestehenden zentralen Datenbankserver bereitgestellt. Sie unterliegen damit dem Management dieses Servers. Dieser Server wird regelmäßig gepatcht und upgegradet. Diese ressourcen- und kostensparende Variante ist, wenn möglich, immer zu bevorzugen. Auf diesem Server gibt es eine zentrale Standardinstanz (Default Instanz), auf der in der Regel alle Datenbanken liegen. Nur im Sonderfall und mit ausführlicher Begründung kann auch eine eigene Instanz für diverse Datenbanken angelegt werden. Darüber hinaus gibt es außerdem noch eine Testinstanz für benötigte Testdatenbanken.

Bei der Beantragung sind geeignete Rahmenparameter zu benennen, die es der Fachabteilung ermöglichen, das System zu bemessen, um die notwendigen Ressourcen zur Verfügung zu stellen. Die Datenbank wird standardmäßig auf einem zentralen virtualisierten Server zur Verfügung gestellt. Die Lizensierung übernimmt die FSG. Die Lizenzkosten werden der jeweiligen Kostenstelle belastet.

ORACLE

Falls benötigt, können bei der FSG auch ORACLE Datenbanken eingesetzt werden.

Diese werden in der Regel auf einem bestehenden zentralen ORACLE Datenbankserver zur Verfügung gestellt. Sie unterliegen damit dem Management dieses Servers. Dieser Server wird regelmäßig gepatcht und upgegradet. Diese ressourcen- und kostensparende Variante ist, wenn möglich, immer zu bevorzugen. Ausschließlich in sorgfältig begründeten Sonderfällen können ORACLE Datenbanken auch auf eigenständigen Servern betrieben werden.

Bei der Beantragung sind geeignete Rahmenparameter zu benennen, die es der Fachabteilung ermöglichen, das System zu bemessen, um die notwendigen Ressourcen zur Verfügung zu stellen. Die Datenbank wird standardmäßig auf einem zentralen physischen Server zur Verfügung gestellt. Die Lizensierung übernimmt die FSG. Die Lizenzkosten werden der jeweiligen Kostenstelle belastet.

15 Clientsysteme

Die Clients der FSG sollen eine moderne, schnelle und schlanke Arbeitsplattform sein, welche einfach zu verwalten ist.

Als Betriebssystemversion wurde Windows festgelegt. Die verwendete Version ist zu erfragen.

Der Windows Client wird im Rahmen eines Schichtmodells erstellt, dies erlaubt es, wenn nötig, dynamisch und schnell den Windows Client auf neue Bedürfnisse anzupassen. Die drei wesentlichen Schichten sind Basis-Client, Standard-Client und die Fachapplikationen.

Basis-Client

> Beinhaltet alle grundsätzlichen Einstellungen und aktuelle Patches des Betriebssystems und Grundapplikationen, modellabhängige Treiber und die Integration in die FSG-Domäne.

Standard-Client

> Die Schicht Standard Client setzt sich aus der Schicht Basis Client und der als Standard-Applikationen definierten Software zusammen.

Fachapplikationen

> Auf den Plattformen „Basis Client“ und „Standard Client“ können Applikationen aus dem Bereich „Fachapplikationen“ den jeweiligen Clients zugewiesen werden. Die Installation wird mittels Softwareverteilung durchgeführt.

Als Webbrowser wird unternehmensweit der Edge Chromium Browser mit der Installation des Betriebssystems zur Verfügung gestellt. Dieser Browser ist der Standardwebbrowser da viele Unternehmensseiten auf diesen zurechtgeschnitten sind. Zusätzlich wird der Google Chromium Browser installiert. Dieser Browser ist nicht notwendig, kann aber parallel verwendet werden.

Der Client ist durch den Einsatz des Cisco Secure Endpoint gesichert. Die Firewall ist im Unternehmensnetzwerk als auch im privaten Netzwerk aktiviert.

Alle Clients werden mittels Bitlocker verschlüsselt. Das lokale Passwort wird mittels LAPS in 14 Stellen verschlüsselt und wird automatisch aller 30 Tage geändert.

Das Betriebssystem und dafür vorgesehene Applikationen unterliegen einem automatisierten zentralen Patchmanagement.

16 SharePoint-Plattform

Die FSG stellt für ihre Mitarbeiter ein zentrales System zur Kommunikation und Zusammenarbeit zur Verfügung. Dieses basiert auf Microsoft SharePoint, derzeit in der Version 2019.

Dieses System ist der zentrale Arbeitsplatz-Einstiegspunkt für die Informationen und Dienste rund um den Flughafen. Verschiedenste Inhalte werden direkt in der Intranet-Anwendung veröffentlich und sind so allen Beschäftigten zugänglich. Weitere Anwendungen sind direkt vom Intranet aus erreichbar.

Für die interne und externe Zusammenarbeit können Arbeitsräume (SharePoint-Site-Collections) angelegt werden. Für Projekte werden diese automatisiert aus SAP PPM erstellt.

Die systemeigene Suche ist so konfiguriert, dass Seiten, Inhalte und Dokumente vollindiziert werden und an M365 angebunden.

Die Benutzer der Plattform werden zentral über das Active Directory verwaltet. Jeder Benutzer benötigt daher einen AD-Account. Das System ist an den E-Maildienst der FSG angebunden.

Über die integrierte Nintex-Workflowengine können komplexe Prozesse abgebildet werden.

17 Dienste

17.1 Verzeichnisdienst Microsoft Active Directory Domain Service ADDS

Die FSG betreibt ein Verzeichnisdienst auf Basis von Microsoft Active Directory Domain Service (ADDS). Beim Active Directory handelt es sich um einen Verzeichnisdienst von Microsoft für Windows-Netzwerke. Das Active Directory ermöglicht es, die Struktur einer Organisation nachzubilden und die Verwendung von Netzwerkressourcen oder -objekten zentral zu verwalten. Die im AD gespeicherten Objekte werden für die Authentifizierung und Autorisierung verwendet.

17.1.1 AD-Domäne:

Das derzeitige FSG Domänenmodell besteht aus einer Single Root – Single Child-Domäne. Zwischen den beiden Domänen besteht eine transitive bidirektionale Vertrauensstellung. Die AD Struktur lehnt sich an die Organisationstruktur des Flughafens Stuttgart an. Hierzu werden Organisationseinheiten verwendet, welche für die Verwaltung durch die Fachabteilungen delegiert werden.

17.2 Clouddienste:

Der Flughafen Stuttgart nutzt derzeit Microsoft M365 und Azure als Cloudanbieter. Hierbei werden unterschiedliche Clouddienste verwendet, wie:

- Azure AD
- Azure AD Multi Faktor Authentifizierung
- Teams
- Exchange Online
- Planner
- Power Automate
- OneDrive
- …

Werden bei der FSG Prozesse eingeführt, die Clouddienste nutzen, so müssen diese detailliert logisch und technisch beschrieben werden.

17.3 Dateidienste

Die Dateidienste basieren auf einer Microsoft Windows Infrastruktur. Dabei stehen insbesondere die Redundanz und Ausfallsicherheit im Mittelpunkt. Die Redundanz und Ausfallsicherheit werden durch mehrere virtuelle Windows Dateiserver realisiert. Die Bereitstellung der Daten erfolgt mittels DFS (Distributed File System).

Durch die Nutzung von ABE wird gewährleistet, dass die Benutzer nur die Daten und Ordner sehen, auf die sie auch Zugriffsberechtigungen haben.

17.3.1 Microsoft DFS

Das Distributed File System (DFS, englisch für Verteiltes Dateisystem) von Microsoft ermöglicht es, im Rechnernetz verteilte Verzeichnisse zu Verzeichnisstrukturen zusammenzustellen. Die Verzeichnisse können sich auf unterschiedlichen Datenspeichern befinden und erscheinen Benutzern dennoch als geschlossene Struktur.

Die Topologie des DFS umfasst ein Verzeichnis als DFS-Stamm und Verknüpfungen auf die Zielverzeichnisse. Es ist ein Domänenintegrierter DFS-Stamm mit dem Namen „DFS.FSG“ verfügbar. Der komplette DFS-Stamm ist als \\fsg.airport-stuttgart\DFS.FSG definiert und wird als Laufwerk W: zur Verfügung gestellt.

Alle Verzeichnisse unterschiedlicher Server welchen Usern zur Verfügung gestellt werden sollen werden über das DFS veröffentlicht und verwenden den gemeinsamen Einstiegspunkt.

Das DFS der FSG ist ausfallsicher konzipiert.

17.4 Druckdienste

Der Druckdienst ist ein zentraler Verwaltungspunkt zum Freigeben von Druckern in einem Netzwerk und zum Verwalten von Druckerserver- und Netzwerkdruckeraufgaben. Alle Netzwerkdrucker werden über eine Microsoft Printserverinfrastruktur zur Verfügung gestellt. Alle Druckaufträge werden über diese Infrastruktur an die entsprechenden Drucker verteilt.

17.5 Domain Name Service (DNS)

Das Domain Name System (DNS) ist einer der wichtigsten Dienste im Netzwerk und ein elementarer Bestandteil eines funktionierenden ADDS.

Das zurzeit eingesetzte DNS ist auf Basis Microsoft Windows Server installiert.

Für alle durch die FSG betriebenen Netzwerkhosts muss eine Namensauflösung auf Basis von DNS möglich sein. Alle Hosts die bei der FSG zum Einsatz kommen müssen in der entsprechenden Zone eingetragen sein. Der DNS-Service bei der FSG basiert auf einer Root uns Sub-Domain Konfiguration. Die Hosteinträge der aller Netzwerkclients werden standardmäßig in der Subdomain angelegt. Die Root Domäne dient der Vereinfachung der Namensauflösung der Hosteinträge. Dor werden hauptsächlich Aliasnamen der Hosts angelegt. Das Anlegen eine DNS-Subdomain ist immer zu Begründen und Bedarf eine Zustimmung über den Change-Prozess.

DNS-Clientcomputer (Domain Name System) können dynamische Updates verwenden, um ihre Ressourceneinträge auf einem DNS-Server zu registrieren und dynamisch zu aktualisieren, sobald Änderungen auftreten. Die dynamischen Updates sind so konfiguriert, dass nur sichere Updates durchgeführt werden. Das bedeutet, dass der Client Mitglied des AD der FSG sein muss. Ist diese Voraussetzung nicht gegeben muss der Eintrag manuell erfolgen ebenso wie alle Änderungen an diesem Eintrag.

DNS Anfragen, die sich auf Geräte beziehen, die nicht durch die FSG DNS Server gehostet werden, werden weitergeleitet.

Mit Umbrella wurde von Cisco das erste Secure Internet Gateway (SIG) in der Cloud bereitstellt. Mit dieser Lösung von Cisco ist sicher, dass sich Ihre mobilen Mitarbeiter fernab des Firmennetzes, geschützt mit Internet und Cloudanwendungen verbinden.

Alle Clients, welche mit dem Secure Client ausgestattet sind, müssen auf die Windows AD DNS Server geleitet werden. In der Regel werden die DNS Server per DHCP verteilt. Clients ohne Secure Endpoint/Umbrella wie z.B. eine SPS oder andere IoT Geräte müssen die Umbrella DNS Server eingetragen bekommen.

17.6 Zentraler Zeitgeber (NTP)

Die FSG betreibt einen zentralen Zeitserverdienst für die Domänencontroller und alle nicht domänenzugehörigen Systeme.

Für Windowssysteme in der Domäne wird die Domänenhierarchie basierende Synchronisation verwendet. Alle Windows-Clients und Windows-Server werden über die Domänencontroller der Domäne STRAERO synchronisiert. Für diese Clients/Server sind keine weiteren Konfigurationen notwendig und zulässig.

Alle nicht domänenzugehörige Systeme sind so zu konfigurieren das sie ihre Zeit über den zentralen Zeitserverdienst der FSG beziehen. Der aktuell verfügbare Zeitserver kann über das ServiceCenter angefragt werden.

Das Bereitstellen von weiteren Zeitservern bzw. NTP-Diensten im Netzwerk der FSG ist nicht gestattet.

Alle eingesetzten Zeitsynchronisationsmechanismen müssen den aktuellen Richtlinien der IETF RFC entsprechen (z.Zt. RFC1305, RFC2030)

18 Namenskonventionen

Die Erneuerung und Neustrukturierung der Infrastruktur der FSG, machte es erforderlich, dass auch künftig eindeutig normierte Standards zur Benennung der Bestandteile der Infrastruktur geschaffen werden. Diese werden im Dokument „Namenskonvention“ regelmäßig aktualisiert.

Hierbei sind nicht nur hardwarespezifische (Server, Clients, Drucker…), sondern auch logische Bestandteile (Organisationseinheiten, Gruppen, GPOs, …) der Infrastruktur zu betrachten.

19 Adminkonzept

Allgemeine Vorgaben an die administrativen Konten bei der FSG

19.1 Ein Benutzerkonto hat niemals administrative Rechte

Wenn es Ausnahmen geben muss, müssen diese über eine Maßnahme mit Begründung und einen Change von den Security verantwortlichen (Abt. FP) genehmigt werden. Liegt diese Genehmigung vor, werden die administrative Rechte nicht dem Benutzerkonto zugewiesen, sondern ein dediziertes administratives Konto angelegt und die entsprechenden Rechte diesem Konto zugewiesen. Diese Festlegung gilt für alle administrativen Aufgaben unabhängig von der Art und der Ausprägung der administrativen Berechtigungen.

19.2 Personalisierte Administratorenkonten

Jeder Benutzer mit administrativen Aufgaben bekommt ein zusätzliches administratives Konto gemäß der Namenskonvention der FSG.

Die Zuweisung der administrativen Berechtigungen geschieht nach Möglichkeit nur über Admin-Gruppen. Das Konto darf nur für administrative Zwecke genutzt werden. Dieses Konto hat kein Anmeldeskript, kein Profil, kein E-Mailpostfach.

20 Planungshandbuch Passive IT Infrastruktur

Das Planungshandbuch "Passive IT Infrastruktur " dient als verbindliches Regelwerk für die Liegenschaften der Flughafen Stuttgart GmbH einschließlich aller Tochterunternehmen. Das Regelwerk findet immer dann Anwendung, wenn im Rahmen einer Sanierungsmaßnahme oder eines Neubauprojekts Fernmelde- LWL- und anwenderneutrale Kommunikationsnetze ausgetauscht bzw. neu errichtet werden sollen. Abweichungen oder Äderungen bedürfen der schriftlichen Zustimmung der Fachabteilung FB am Flughafen Stuttgart.

Die Hauptaufgabe des Kabelhandbuchs besteht darin, einen einheitlichen Standard

für alle Liegenschafen der Flughafen Stuttgart GmbH zu sichern und eine zukunftsfähige

Infrastruktur der Fernmeldeanlagen und für ein anwenderneutrales Kommunikationsnetzwerk

zur Verfügung zu stellen.

Sollten im Rahmen einer Planungsaufgabe Widersprüche zwischen den Anforderungen

aus dem Kabelhandbuch und der Planungsaufgabe bestehen, sind diese schriftlich

über die Projektleitung anzumelden und vor dem Erstellen eines

Leistungsverzeichnisse bzw. einer Beauftragung zu klären.

21 Netzwerkinfrastruktur (AKN)

21.1 Allgemein

Die Netzwerkinfrastruktur der Flughafen Stuttgart GmbH (FSG) wird als Anwenderneutrales Kommunikationsnetzwerk AKN bezeichnet. Die derzeit laufende Version des AKNs ist das AKN IV. Das AKN IV basiert auf einer mandantenfähigen Netzwerkinfrastruktur die auf einer gemeinsamen Hardware Infrastruktur die Ausbildung von unterschiedlichen unabhängigen Mandanten (Kunden) ermöglicht, ohne dass hier eine direkte Kommunikationsbeziehung zwischen den Mandanten besteht.

Über diese Netzwerkinfrastruktur wird innerhalb der Mandanten die Kommunikation z.B. zwischen Server und Client Anwendungen ermöglicht. Das Netzwerk kann hier eine Vielzahl von unterschiedlichen Netzwerkservices transportieren und den Anwendern / Kunden auf dem Campus bereitstellen.

Die Netzwerkinfrastruktur basiert auf Komponenten des Herstellers Cisco Systems, die in einer homogenen, standardisierten, redundanten und modularen Bauweise in den Campus der FSG und in dessen Gebäuden integriert und aufgebaut sind. Die modulare Bauweise beinhaltet hierbei folgenden Module / Bereiche

- Core Modul / Bereich
- Distribution Modul / Bereich
- Access Modul / Bereich
- DataCenter Modul / Bereich
- Firewall Modul / Bereich

Durch den modularen und standardisierten Aufbau der Bereiche kann jederzeit eine Erweiterung bzw. Anpassung der Netzwerkinfrastruktur erfolgen.

Die Module sind bis auf den Access Bereich in sich redundant aufgebaut, so dass ein Ausfall von Teilkomponenten oder Modulbereichen keinen Gesamtausfall des Netzwerkes bzw. der darauf laufenden Services bedeutet.

21.2 Physikalischer Aufbau

Der physikalische Aufbau der Netzwerkinfrastruktur orientiert sich an der Gebäudestruktur auf dem Campus der FSG. In größeren Gebäuden ist ein Distribution Modul / Bereich aufgebaut, an dem dann die jeweiligen Access Module / Bereiche des Gebäudeversorgungsbereiches angebunden sind. Das Distribution Modul kann entweder „nur“ das Gebäude selbst umfassen oder er nimmt auch angegliederte „kleinere Gebäude“ in die Distribution Versorgung auf.

Die jeweiligen Access Module / Bereiche sind redundant über getrennte Trassenführung an das Distribution Modul angebunden.

In folgenden Gebäuden wurden Distribution Module / Bereiche aufgebaut

Core / Distribution Bereich
SkyOffice (SAO)
VL + OPS
LVT + Terminal 4
Feuerwehr
Terminal 1
Terminal 3
Werkstatt
Skyport
Skyloop

Tabelle 1: Distribution Module

Alle Distribution Module / Bereiche sind über redundante Strecken an das Core Modul / Bereich angebunden.

Das Core Modul ist in sich ebenfalls redundant und verteilt an den zwei Standorten im RZ2 im P4 und im Terminal 3 aufgebaut.

Jedes Distribution Modul ist über getrennte Wege / Trassen in zwei unterschiedlichen Gebäuden an das Core Modul angeschlossen.

Das Core Modul selbst ist ebenfalls über getrennte Wege / Trassen redundant untereinander verbunden, um den notwendigen Ausfallschutz für das Modul bzw. für die Backbone Kommunikation gewährleisten zu können.

An das Core Modul ist ebenfalls über getrennte Wege / Trassen redundant das Firewall Modul angebunden.

Das Firewall Modul stellt den zentralen Übergang zum Internet und den Internet Services, als auch zu den mandantenübergreifenden Kommunikationsmöglichkeiten bereit.

Als letztes ist an das Core Modul über getrennte Wege / Trassen das DataCenter Modul angebunden.

Das DataCenter Modul beinhaltet die zentrale Computing und Storageinfrastruktur für die Mandanten in der Netzwerkinfrastruktur des AKN IV. Die Verteilung des Moduls ist in den beiden Rechenzentren im P4 und im Tower.

Nachfolgendes Übersichtsbild zeigt den physischen Aufbau der Netzwerkinfrastruktur

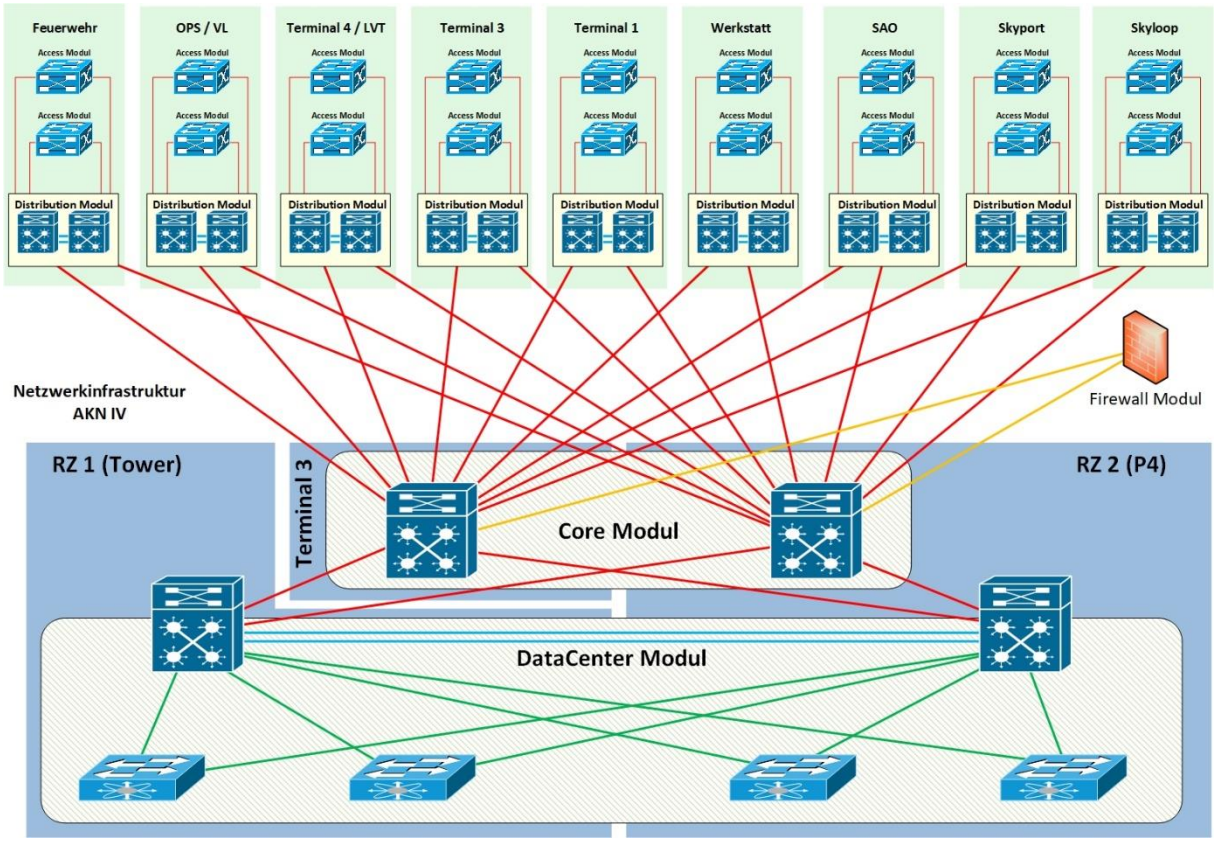

Abbildung 3 FSG Netzwerkinfrastruktur

21.2.1 Beschreibung Core Modul

Das Core Modul ist mit 2 Cisco 9600 Switchen, die mittels dem Virtual Switching System (VSS) zu einem logischen Switch (Virtual Chassis) zusammengeschaltet sind, aufgebaut. Die jeweiligen Switche des VSS Systems befinden sich im RZ 2 im P4 und im Terminal 3.

21.2.2 Beschreibung Distribution Modul

Die Distribution Module sind jeweils mit 2 Cisco 9500 Switchen, die mittels dem Virtual Switching System (VSS) zu einem logischen Switch (Virtual Chassis) zusammengeschaltet sind, aufgebaut. Die Anbindung des Distribution VSS Systems an das Core Modul erfolgt über einen Etherchannel mit 4 x 25Gbit Verbindungen, aufgeteilt in Richtung der beiden RZ Standorte.

21.2.3 Beschreibung Access Modul

Die Access Module sind jeweils mit den Cisco Switchen aus den Serien 9300, 3000 IE, 2000 IE, 4000 IE, 4010 IE, 3560CX und 38xx aufgebaut. Die Module stellen den Endgeräte Port für die Mandanten bzw. dessen Netzwerkendgeräte zur Verfügung. Jedes Modul deckt einen Versorgungsbereich innerhalb des Gebäudes oder einer zugehörigen Gebäudeerweiterung ab. Der Versorgungsbereich orientiert sich hier anhand der Vorgaben der strukturierten Verkabelung nach EN 50173.

Das Modul wird als einzelner Switch bis hin zu einem Stack aus mehreren Switches aufgebaut. Durch die Ausbildung als Stack ist eine Komponentenredundanz innerhalb des Moduls gewährleistet. Das Modul ist je nach Portanzahl mit mindestens einem EtherChannel mit 2 x 1Gbit an das Distribution Modul angebunden. Bei Portanzahlen > 100 erfolgt die Anbindung über mindestens 4 x 1Gbit. Hierbei werden die einzelnen Verbindungen über getrennte Wege / Trassen auf die beiden Switche des Distribution VSS verteilt angebunden.

21.2.4 Beschreibung DataCenter Modul

Das DataCenter Modul ist durch Cisco Catalyst 6880 Switche und durch Cisco Nexus 5548 Switche in Verbindung mit Cisco Nexus 2248TP-E Fabric Extendern (FEX) aufgebaut. Hierbei bilden die beiden Catalyst 6880 Switche im VSS als Virtual Chassis aufgebaut ein quasi eigenständiges Distribution Modul für den DataCenter Bereich.

An diesem DataCenter Distribution Modul sind dann pro RZ jeweils 2 x Nexus 5548 Switche angeschlossen. Die Nexus Switche innerhalb eines RZs sind über einen virtual Port-Channel (vPC) ebenfalls zu einem Virtual Chassis (Bezeichnung vPC Domain) zusammengeschlossen. Diese vPC Domäne wird über 4 x 10Gbit, jeweils 2 x 10Gbit pro Nexus 5548 Switch, voll redundant an das DataCenter Distribution Modul angebunden. Somit stehen pro RZ 40Gbit Bandbreite für die Anbindung der DataCenter Computing Infrastruktur zur Verfügung.

In Richtung der Computing Infrastruktur Hardware in Form der Serversysteme werden die Nexus 2248TP-E FEXen als Anschlusspunkt in den Schrankreihen eingesetzt. Die FEXe bieten 48 x 1 Gbit Cu Ports zur Anbindung der DataCenter Computing Hardware. Jede FEX ist mit 4 x 10Gbit an einen Nexus 5548 Switch angebunden. Die FEXe in den Schrankreihen werden immer paarweise aufgebaut um eine redundante Anbindung der Computing Hardware über die FEXe an die Nexus 5548 realisieren zu können. Nachfolgendes Übersichtbild zeigt den Aufbau

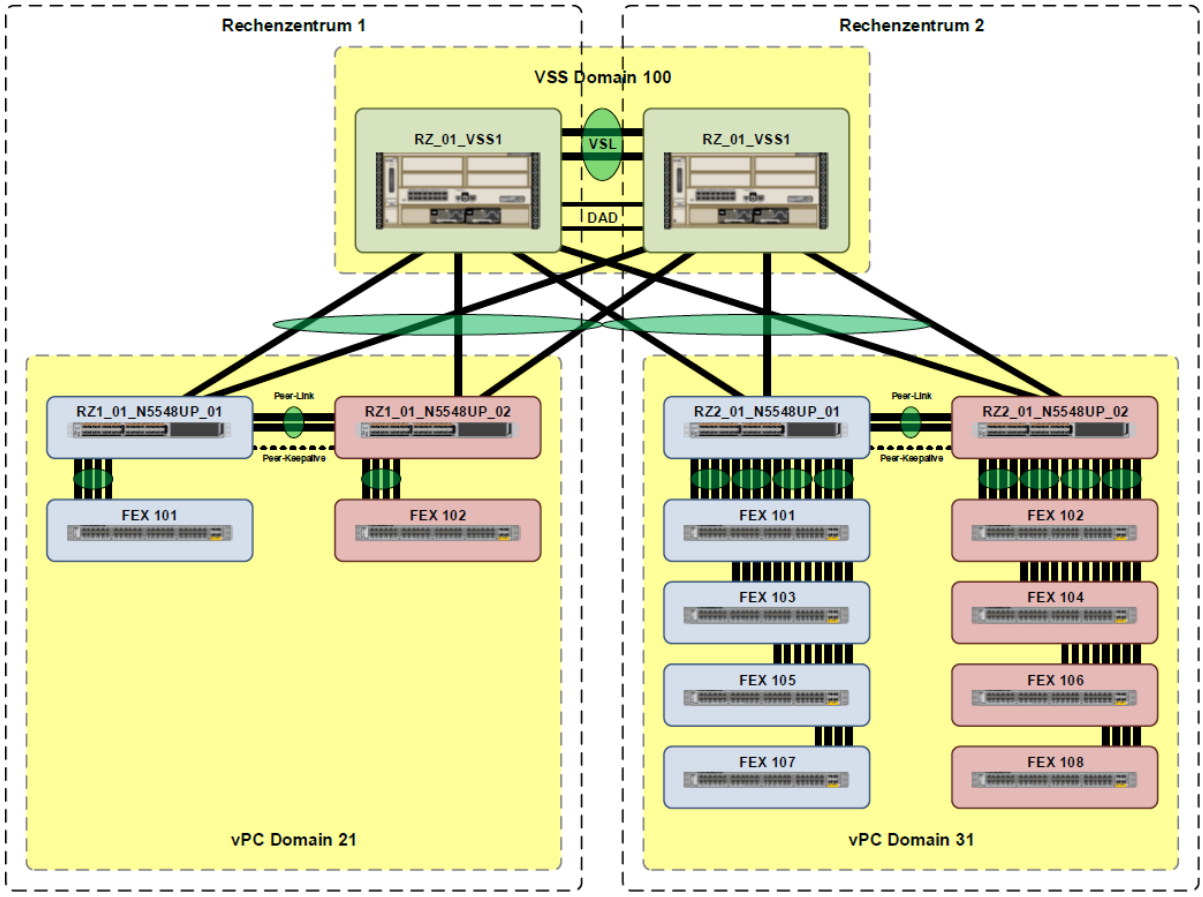

Abbildung 4 Übersichtsbild physisches DataCenter Modul

21.2.5 Beschreibung L2 Kunden / Sondernetze

Neben dem oben beschriebenen Aufbau mit den dargestellten Verbindungen gibt es parallel für bestehende Layer 2 Kundenumgebungen und Sondernetze eine zusätzliche physische Verkabelung

um auf dem Campus der FSG gebäudeübergreifend flache Layer 2 Netzwerke bereitstellen zu können.

Diese Bereitstellung ist ein Restbereich aus der AKN III Generation und wird sukzessive in die mandantenbezogene Bereitstellungsmethode der AKN IV Generation umgestellt. Ein weiterer Ausbau dieser Strukturen ist nicht geplant.

Zum Aufbau dieser flachen Layer 2 Struktur sind die Distribution Module, auch das DataCenter Distribution Modul, mit einem separaten Etherchannel mit 2 x 10Gbit miteinander verbunden.

21.2.6 Physische Netzwerkinfrastruktur durch die Virtual Chassis Funktionen

Bedingt durch die Virtual Chassis Technologie mittels VSS und der vPC Domänen kann das Übersichtsbild, trotz des Einsatzes von redundanten Verbindungsstrecken auf getrennten Trassen und dem Aufbau in unterschiedlichen Gebäuden, vereinfacht dargestellt werden. Dies zeigt das nachfolgende Übersichtsbild

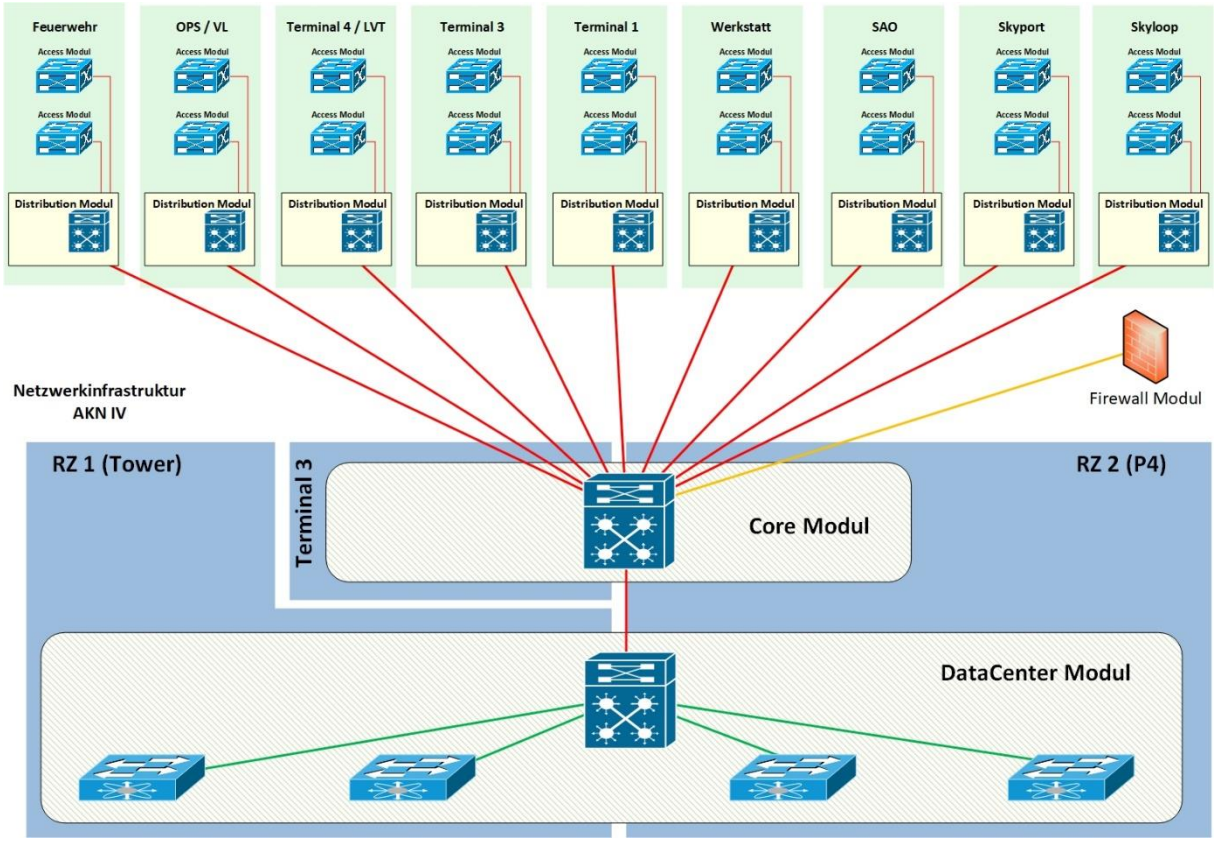

Abbildung 5 physische Netzwerkinfrastruktur durch die Virtual Chassis Funktionen

21.3 Logischer Aufbau

21.3.1 Allgemein

Auf dem unter Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** beschriebenen physischen Aufbau der Netzwerkinfrastruktur wird die nachfolgende logische Infrastruktur aufgesetzt und betrieben. Sie gliedert sich grundsätzlich in eine mandantenbezogene Implementierung von Kundenanforderungen an die physische Netzwerkinfrastruktur.

Unter der mandantenbezogenen Implementierung ist eine jeweils kundenbezogene logische Infrastruktur zu verstehen, die ohne zusätzliche externe Konfiguration über das Firewall Modul keine

Kommunikation über die Mandantengrenzen hinaus ermöglicht. D.h. es wird eine sichere und geschützte Kommunikation innerhalb des Mandanten ermöglicht, die keinem Einfluss oder einer Sichtbarkeit aus bzw. durch die anderen Mandanten ausgesetzt ist.

21.3.2 Aufbau Mandanten Struktur

Zur Erfüllung dieser Mandanten-Struktur ist auf der physischen Netzwerkinfrastruktur ein Layer 3 Multi Protokoll Label Switching (MPLS) Netzwerk implementiert. Im Gegensatz zu einem Standard Design eines Layer 3 MPLS Netzwerkes werden innerhalb der Struktur ausschließlich MPLS Provider Edge-Router (PE-Router) eingesetzt. Die PE-Router werden in den Distribution Modulen, im DataCenter Distribution Modul und im Core Modul implementiert. Nachfolgendes Übersichtbild zeigt den Aufbau.

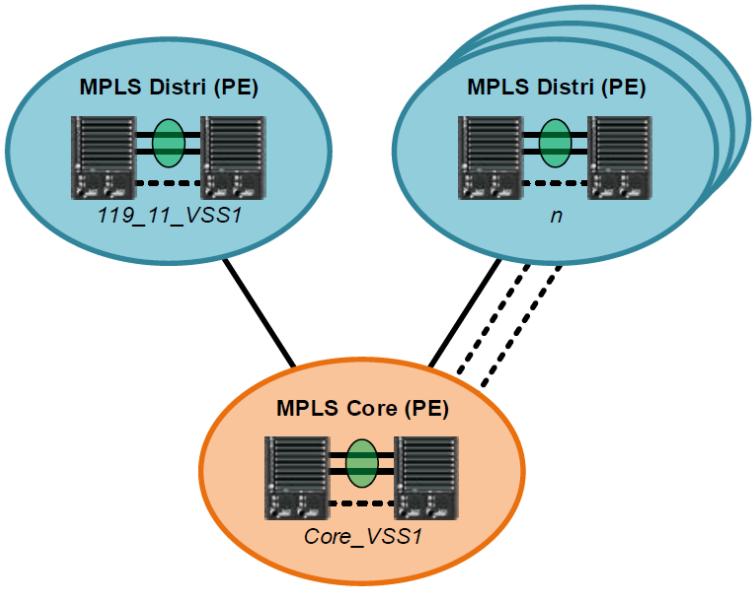

Abbildung 6 Aufbau Layer 3 MPLS Netzwerk

Innerhalb des Layer 3 MPLS Netzwerkes wird als Routingprotokoll OSPF und BGP eingesetzt. Hierdurch sind die redundanten Kommunikationswege für die mandantenbezogenen Labelswitchingpakete gewährleistet.

Damit keine Kommunikation innerhalb der gerouteten Instanzen zwischen den Mandanten möglich ist, wird jeder einzelne Mandant mittels Virtual Routing an Forwarding (VRF) voneinander getrennt. Jeder VRF hat einen sogenannten Route Distinguisher (RD) der für das mandantenbezogene Labeling der Pakete innerhalb des MPLS Netzwerkes zuständig ist. Als Labelprotokoll wird das Label Distribution Protokoll (LDP) eingesetzt. Nachfolgendes Übersichtsbild zeigt die schematische Trennung der einzelnen VRF Mandanten mit den zugehörigen RDs die innerhalb der MPLS Wolke mit dem zugehörigen Label geswitched werden.

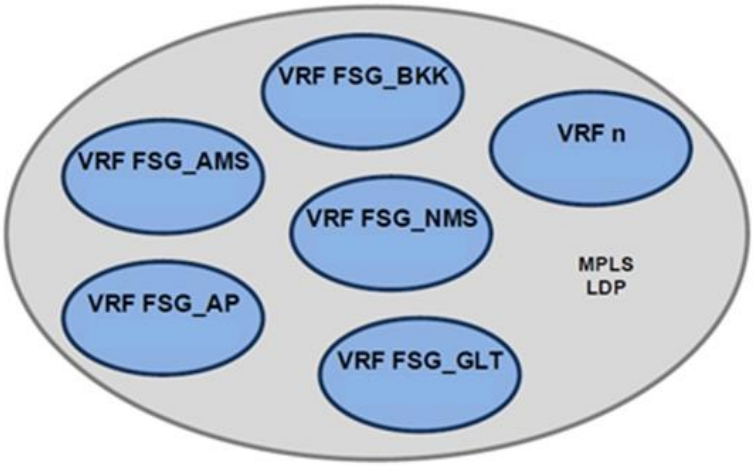

Abbildung 7 Darstellung VRF Mandanten

Am Rande des Layer 3 MPLS Netzwerkes (an den PE-Routern) erfolgt der Übergang auf die jeweilige mandantenbezogene Layer 2 Struktur innerhalb der Versorgungsbereiche der Distribution Module bzw. in den zugehörigen Access Modulen.

Diese Layer 2 Struktur wird mit mandantenbezogenen VLANs realisiert, die je nach Ausprägung (Größe) des Mandanten pro Access Modul oder Access Modul übergreifend eingesetzt werden.

Somit erfolgt außerhalb des Layer 3 MPLS Netzwerkes die Trennung zwischen den Mandanten auf Basis virtueller Netze (VLANs). Die VLANs werden in den Distribution Modulen direkt der zugehörigen VRF Instanz zugeordnet.

21.3.3 Übergreifende Kommunikation

Mandantenübergreifende Kommunikationen oder z.B. Kommunikationen in Richtung von zentralen Diensten (zentraler Internetzugang oder zentrale DHCP Services) werden nur durch das Firewall Modul und dessen virtuelle Firewalldienste zur Verfügung gestellt. Nachfolgendes Übersichtsbild zeigt den Zusammenhang.

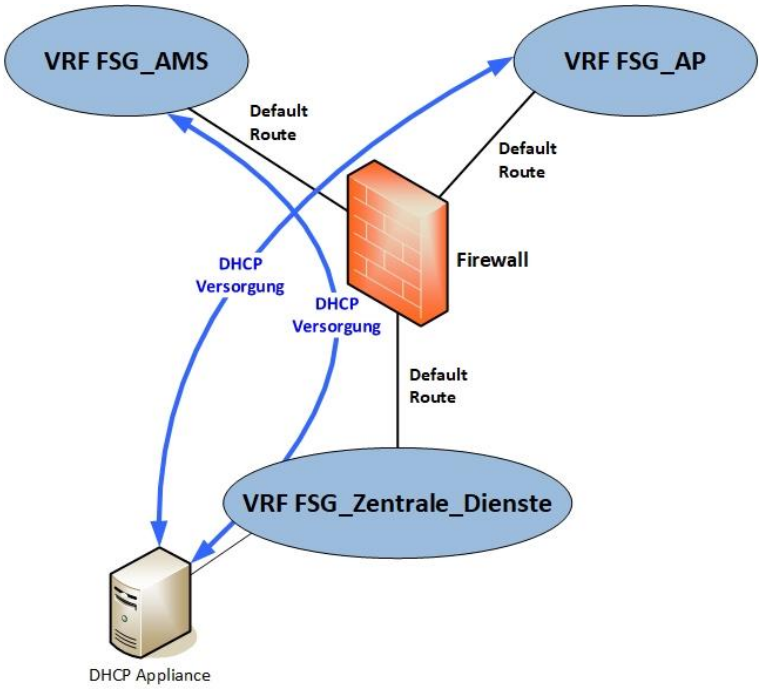

Abbildung 8 Übersichtsbild mandantenübergreifende Kommunikation

Durch den Netzwerkaufbau und die Implementierung der MPLS PE_Router in den Distribution Modulen können Mandantenstrukturen flächendeckend auf dem gesamten Campus bis hinein in das DataCenter Modul abgebildet und aufgebaut werden.

Kunden der FSG haben hierdurch die Möglichkeit auch weit verteilte Bereiche Ihres Netzwerkes sicher und einfach exklusiv miteinander zu verbinden.

21.3.4 Sonderbereich Layer 2 Netzwerk

Als Sonderbereich, wie unter Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** beschrieben, ist derzeit noch parallel zum Layer 3 MPLS Netzwerk eine flache Layer 2 Netzwerklösung im Einsatz, die über die Distribution und Access Module hinweg exklusive VLANs bereitstellen kann. Eine Kommunikation zwischen den VLANs ist ebenfalls, wie bei den MPLS Mandanten, nur über die Datacenter Firewall möglich. Hierdurch werden noch spezielle Kundensituationen aus der vorherigen AKN III Version und Sonderlösungen für Netzwerkdienste abgebildet.

21.3.5 Strukturierung / Einteilung der Mandanten Strukturen

Da nicht alle Netzwerk Anforderungen auf dem Campus der FSG durch die Kunden gleich sind wird bei der Einteilung der Kunden zu den Mandanten Strukturen in folgende Bereiche unterschieden ´´.

- Kleiner Layer 3 Mandant
- Großer Layer 3 Mandant
- Sondernetz (Layer 2)

- Kundennetz (Layer 2) (Rückbau geplant)

Eine Sonderstellung nimmt noch der Basis Mandant der FSG der „FSG_Office“ Mandant ein, welcher die Grundversorgung der FSG mit Office Netzwerkservices auf dem gesamten Campus sicherstellt.

Für die Layer 3 Mandanten wird ein Netzwerk, welches über die Layer 3 MPLS Infrastruktur bereitgestellt wird, aufgebaut und integriert.

Die wesentliche Unterscheidung zwischen kleinen und großen MPLS Mandanten erfolgt in Bezug auf Ihre Größe auf dem FSG Campus und der räumlichen Verteilung innerhalb des Versorgungsbereiches in den Distribution-Modulen. Folgende Definition wurden hier zur Aufteilung festgelegt.

- Kleine Layer 3 Mandanten erhalten max. ein VLAN in den Distribution Modulen. Dieses VLAN kann sich über mehrere Access Module innerhalb des Distribution Moduls erstrecken.
- Große Layer 3 Mandanten können theoretisch max. 32 VLANs pro Distribution Modul bereitgestellt werden. Die tatsächliche Anzahl orientiert sich an der Anzahl der Access Modulen / an den vorhandenen Verteilern in den jeweilig versorgten Distribution-Bereichen.
- Sondernetze (Layer 2) erhalten ein VLAN welches auf dem gesamten Campus Distribution- und Access-Modul übergreifend durch die parallele flachen physische Layer 2 Infrastruktur aufgebaut und integriert werden kann.
- Kundennetz (Layer 2) erhalten ebenfalls ein VLAN vergleichbar wie in den Sondernetzen (Layer 2)

Nachfolgendes Übersichtsbild zeigt den Unterschied zwischen kleinen und großen Mandanten.

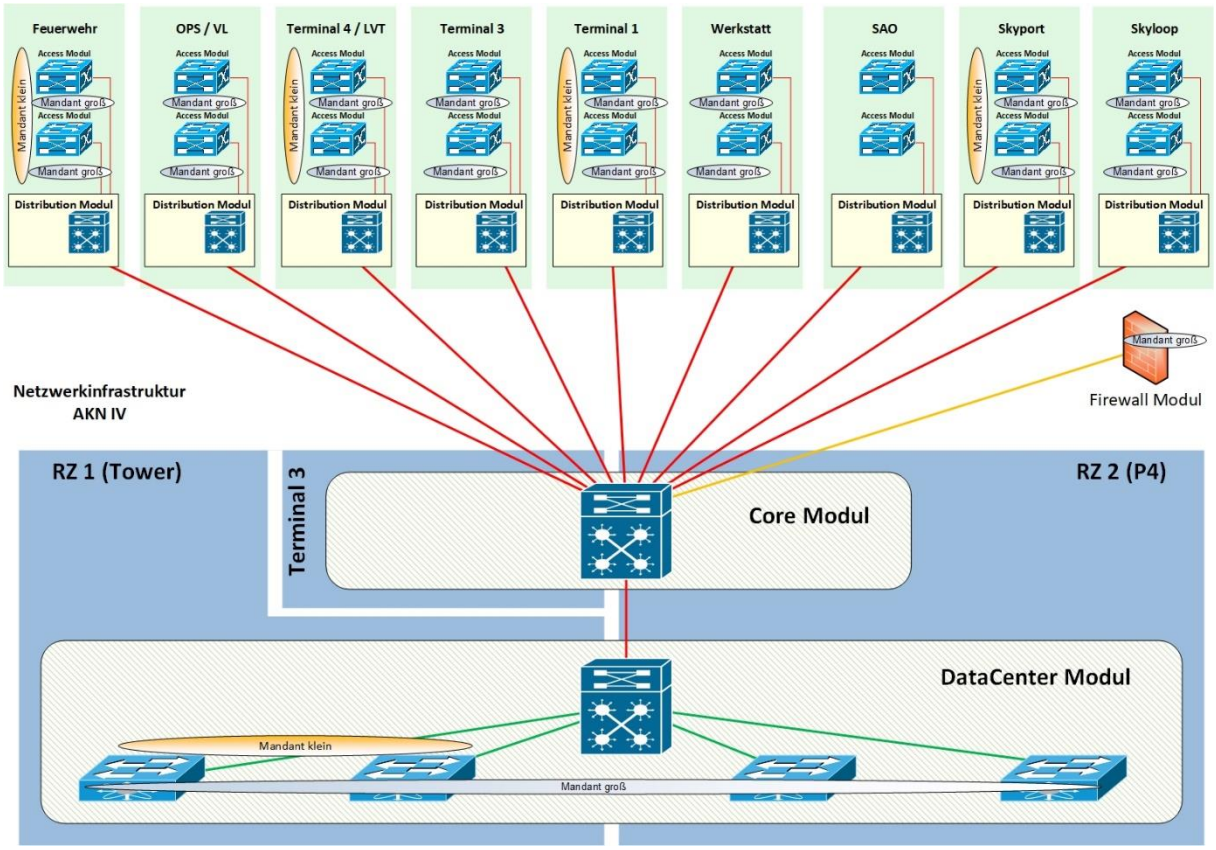

Abbildung 9 Übersichtsbild mandantenübergreifende Kommunikation

21.4 Adressierungskonzept der Mandanten

21.4.1 FSG Basis Mandant (FSG_Office)

Wie beschrieben wird für die IT technische Grundversorgung des Campus mit allen Gebäuden auf dem Netzwerk der Basis Mandant FSG_Office betrieben. Dieser wird in allen Access Modulen über 2 getrennte VLANs redundant zur Verfügung gestellt. Für die Adressierung wird nachfolgende Struktur verwendet.

Der Adressraum des Mandanten wurde im privaten Adressierungsbereich 10.0.0.0 mit dem Bereich 10.96.0.0/14 festgelegt. Hierdurch stehen grundsätzlich ca. 260.000 IP Adressen für zur Verfügung.

Für die Strukturierung wurde dieser /14er Adressraum entsprechend der gebildeten Core- und Distribution Module nochmals unterteilt. Hierdurch entstanden nachfolgende Adressbereiche

Core / Distribution Bereich	Netz-ID
Backbone	10.96.0.0
Zentrale Dienste / DataCenter	10.96.64.0
Reserve	10.96.128.0
SkyOffice-Gebäude (SAO)	10.96.192.0
VL + OPS Gebäude	10.97.0.0
LVT-Gebäude + Terminal 4	10.97.64.0
Feuerwehr-Gebäude	10.97.128.0
Terminal 1	10.97.192.0
Werkstatt-Gebäude	10.98.0.0
Terminal 3	10.98.64.0
Reserve	10.98.128.0
Reserve	10.98.192.0
Reserve	10.99.0.0
Skyport	10.99.64.0
Skyloop	10.99.128.0
Reserve	10.99.192.0

Tabelle 2: Adressbereiche der Distribution Module

Nachfolgendes Übersichtsbild zeigt die Strukturierung und Verteilung der Adressbereiche

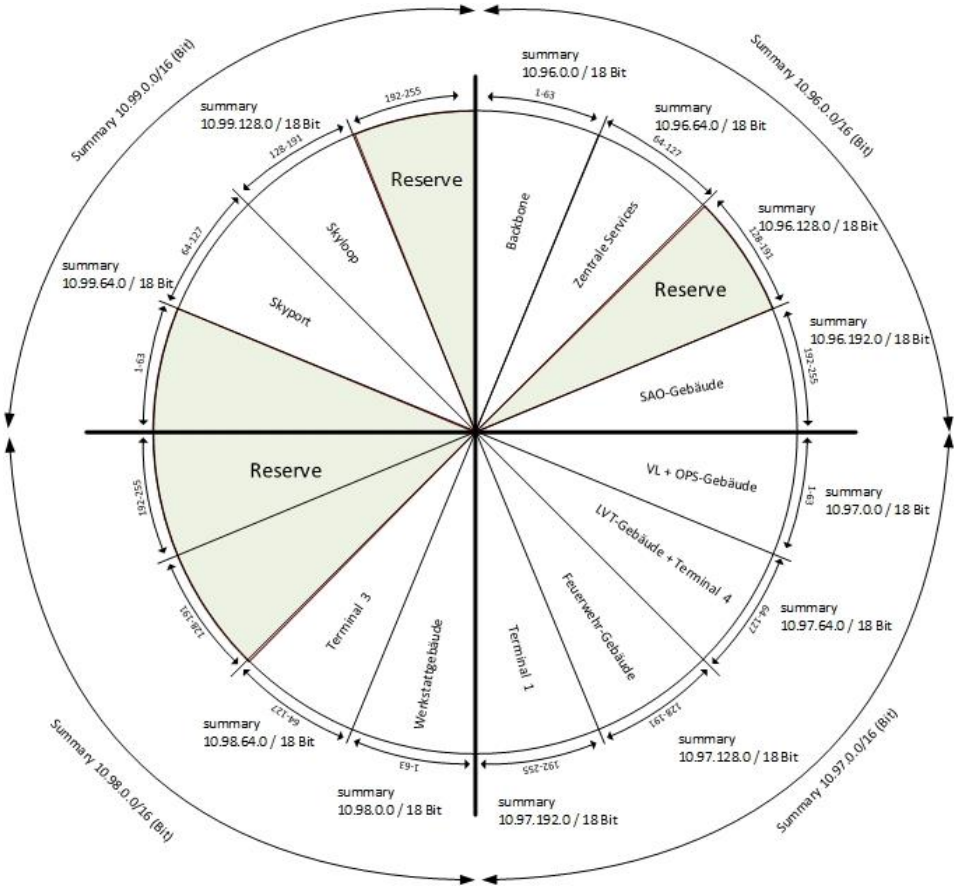

Abbildung 10 Adressbereichs-Diagramm

Wie oben dargestellt wird aus Redundanzgründen und zur optimierten Verteilung der Datenströme in den jeweiligen Access Modulen immer 2 Adressbereiche (VLANs) aufgebaut. Hierzu wurde der /18 Adressraum nochmals unterteilt um 2 Address ID Bereich zu erhalten. Die Vorgehensweise wird nachfolgend am derzeitigen Adressraum 10.96.192.0 /18 (SkyOffice) dargestellt

Bezeichnung	Adress-Bereich	Summary Adresse
SkyOffice	10.96.192.0 - 10.96.254.254	10.96.192.0/18
Bereich Teil1	10.96.192.0 – 10.96.223.254	10.96.128.0/19
Bereich Teil2	10.96.224.0 – 10.96.255.254	10.96.160.0/19

Tabelle 3: Bereichsstrukturierung

Im folgenden Bild ist die Aufteilung der Bereiche nochmals grafisch dargestellt:

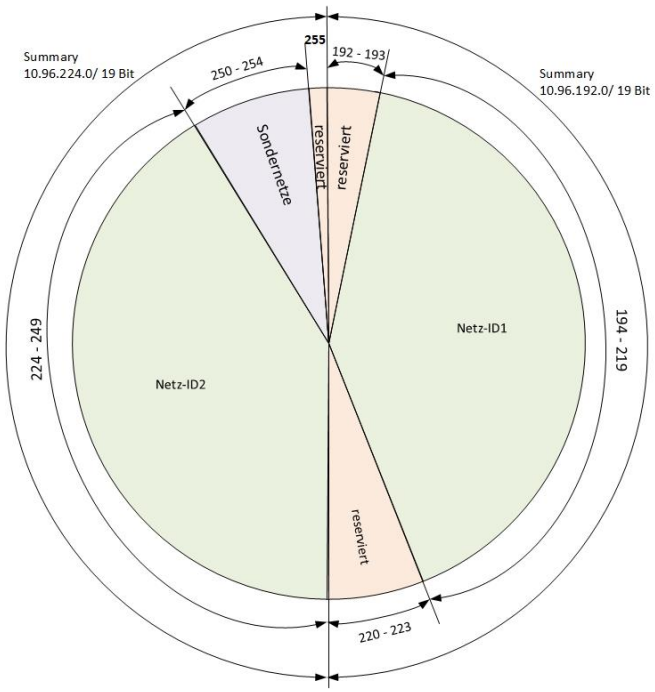

Abbildung 11 Bereichsunterteilungs-Diagramm

21.4.2 Layer 3 Mandant

Grundsätzlich wurde der Adressraum für die Layer 3 Mandanten aus dem Adressbereich ab **10.200.x.x** festgelegt.

Diese werden wie folgt verteilt.

21.4.2.1 Kleine Layer 3 Mandanten

Pro kleinem Layer 3 Mandant wird pro Distribution-Bereich ein Class-C Netzwerk bereitgestellt. Die Distribution-Bereiche sind wie folgt vergeben.

Core / Distribution Bereich	Netz-ID
Backbone	10.217.x.0
Reserve	10.201.x.0
SkyOffice-Gebäude	10.203.x.0
VL + OPS Gebäude	10.205.x.0
LVT-Gebäude + Terminal 4	10.207.x.0
Feuerwehr-Gebäude	10.209.x.0
Terminal 1	10.211.x.0
Werkstatt-Gebäude	10.213.x.0
Terminal 3	10.215.x.0
Skyloop	10.219.x.0
Skyport	10.221.x.0

Tabelle 4: Adressstrukturierung für kleine Layer 3 Mandanten

Der jeweilige Mandant erhält somit die Class-C Netze in den Bereichen

Mandant A erhält pro Distribution Modul immer die Netz ID **10.2xx.1.0**

Mandant B erhält pro Distribution Modul immer die Netz ID **10.2xx.2.0**

Im Rahmen dieser Festlegung sind 255 kleine Layer 3 Mandanten in die Struktur integrierbar. Für eine ggf. erforderliche Erweiterung ist bereits ein weiterer Adressraum reserviert.

21.4.2.2 Große Layer 3 Mandanten

Bei den großen Layer 3 Mandanten werden die Distribution Module gleich wie bei den kleinen Layer 3 Mandanten adressiert. Es werden allerdings die geraden Adressnummern im zweiten Abschnitt verwendet.

Distribution Bereich	Netz-ID
Reserve	10.200.x.0
SkyOffice-Gebäude	10.202.x.0
VL + OPS Gebäude	10.203.x.0
LVT-Gebäude + Terminal 4	10.206.x.0
Feuerwehr-Gebäude	10.208.x.0
Terminal 1	10.210.x.0
Werkstatt-Gebäude	10.212.x.0
Terminal 3	10.214.x.0
Skyloop	10.218.x.0
Skyport	10.220.x.0

Tabelle 5: Adressstrukturierung für große Layer 3 Mandanten

Laut Definition der großen Layer 3 Mandanten müssen hier in den jeweiligen Distribution Modulen mehr Class-C Netze zur Verfügung gestellt werden. Bedingt durch diese Notwendigkeit, wird der jeweilige Distribution Modul Adressbereich (z.B. 10.202.0.x – 10.202.255.x) in 8 Bereiche unterteilt. Somit können in diesem Adressraum max. 8 große Layer 3 Mandanten mit jeweils bis zu 32 Access Modul Adressbereichen bereitgestellt werden.

Mandant A erhält pro Distribution Modul die Netz IDs **10.2xx.0.0 – 10.2xx.31.0**

Mandant B erhält pro Distribution Modul die Netz IDs **10.2xx.32.0 – 10.2xx.63.0**

21.4.3 Sondernetze (Layer 2)

Für die Sondernetze (Layer 2) wird ebenfalls ein privater Adresspool zur Adressierung der flachen Layer 2 VLANs eingesetzt.

Die Adressierung erfolgt aus dem Adresspool **192.168.x.x**

Hierdurch können 255 Netz IDs für die Sondernetze (Layer 2) zur Verfügung gestellt werden.

21.4.4 Kundennetze (Layer 2)

Für die Kundennetze (Layer 2) wird auf eine vorgegebene Adressierung des Netzwerkes bzw. der Netzwerkteilnehmer verzichtet. Hier stellt die FSG ausschließlich ein VLAN zur Verfügung. Die Adressierung wird von den Kunden selbst implementiert.

Einzig bei der Anforderung einer übergreifenden Kommunikation außerhalb des flachen Layer 2 VLANs muss eine Abstimmung und Freigabe der Adressierung mit bzw. durch die FSG erfolgen.

21.5 VLAN Konzept

Analog zur Bereitstellung der Adressbereiche mit den Netz IDs für die Access Module, muss eine Strukturierung und Zuordnung von VLAN IDs erfolgen.

Bei den VLAN IDs wurde bereits ein Ausbau / Erweiterung für die zukünftige Netzwerkstrukturierung vorgesehen. Die bestehenden vergebenen Bereiche zwischen ID 10 – 1199 werden durch die Zugabe der 1000er und 2000er Stelle ergänzt bzw. erweitert. Bei den Erweiterungen wurden eventuelle Überschneidungen z.B. im DataCenter Bereich und im Bereich der FW durch die Ergänzung mit 1000 und 2000 entsprechend beachtet.

Die nachfolgende Aufstellung zeigt die Einteilung der VLANs zu den Mandanten / Kunden Bereichen

Bereichsbezeichnung	VLAN ID	1000er Erweiterung	2000er Erweiterung
DataCenter	10 – 99	Keine Erweiterung	2010 - 2099
Office (FSG)	100 – 399	1200 – 1399	2200 – 2399
APCOA	400 – 410	1400 – 1410	2400 – 2410
Reserve / Frei	411 – 499	1411 – 1499	2411 – 2499
Sondernetze	500 – 550	1500 – 1550	2500 – 2550
Kleine MPLS Mandanten	551 – 599	1551 – 1599	2551 – 2599
Sondernetze L2 Kunden	600 – 699	1600 – 1699	2600 – 2699
Große MPLS Mandanten	700 – 799	1700 – 1799	2700 – 2799
Backbone (Core)	800 – 899	1800 – 1899	2800 – 2899
Reserve / Frei	900 – 999	1900 – 1999	2900 – 2999
Reserviert	1000 – 1099	Keine Erweiterung	Keine Erweiterung
Firewall	1100 – 1199	Keine Erweiterung	2100 – 2199

Tabelle 6: VLAN Strukturierung

21.6 Adressvergabe in den Netz IDs

Die Adressvergabe an die Netzwerkteilnehmer in den jeweiligen Netz ID Bereichen der Access Module werden anhand folgender Festlegungen vergeben.

- Reservierte Adressen für Basis Netzwerkdienste (z.B. Gateway)
- Vergabe von festen IP Adressen
- Vergabe von dynamischen IP Adressen durch den DHCP Dienst
- Vergabe von statischen IP Adressen durch den DHCP Dienst

21.6.1 Reservierte Adressen

In den einzelnen Netz ID Bereichen der Access Modulen ist der Adressbereiche von **x.x.x.1 – x.x.x.20** für die Basis Netzwerkdienste reserviert. Hierunter fallen z.B. das Default Gateway, ggf. ausfallsicher konfiguriert, Loopbackadressen usw.

21.6.2 Feste IP Adressen

Im weiteren Verlauf der einzelnen Netz ID Bereichen ist der Adressbereich von **x.x.x.21 – x.x.x.99** für die manuelle Vergabe von festen IP Adressen an Netzwerkteilnehmer vorgesehen. Hierunter fallen z.B. feste Drucker, Serversysteme etc.

Die Netzwerkeinstellungen müssen auf in den Endsystemen (Netzwerkteilnehmern) vollständig manuell konfiguriert werden.

21.6.3 Dynamische IP Adressen

Der dritte Bereich in den einzelnen Netz IDs ist der Vergabe von dynamischen IP Adressen inkl. aller notwendigen Netzwerkeinstellungen für die Endsysteme (Netzwerkteilnehmer) vorbehalten. Die Vergabe von IP Adressen erfolgt hier im Adressbereich **x.x.x.100 – x.x.x.229**.

Die Vergabe der Adresse erfolgt über das DHCP Protokoll von den zentralen DHCP Netzwerkservices. Die Nutzungsdauer der IP Adresse (Leasetime) ist hierbei auf 5 Tage eingestellt.

Mit der Adressvergabe erhält das Endsystem ebenfalls die Angaben zum Gateway der Netz ID und der DNS Server.

Diese Art der Adressvergabe wird im Wesentlichen bei den Standard Client Endgeräten (PCs / Notebooks / etc.) in den Mandanten eingesetzt.

21.6.4 Statische IP Adressen

Der letzte Adressbereich der einzelnen Netz IDs ist den statischen IP Adressen vorbehalten. Die Vergabe und Zuweisung erfolgt analog dem Verfahren der dynamischen IP Adressen, mit dem Unterschied, dass die jeweiligen Endsysteme (Netzwerkteilnehmer) immer die gleiche IP Adresse durch den DHCP Server zugewiesen bekommen. Hierdurch ist quasi die automatische Zuweisung einer festen IP Adressen an die Endsysteme möglich.

Zur korrekten Anwendung dieses Verfahrens muss im DHCP Dienst eine statische Zuordnung (Reservierung) der MAC Adresse des Endsystems zu einer Adresse aus diesem Adressbereich erfolgen.

Die Vergabe der statischen IP Adressen erfolgt hier im Adressbereich **x.x.x.230 – x.x.x.254**

21.7 DHCP Dienst

Der zentrale DHCP Dienst wird durch ein redundanten Infoblox DHCP Appliance System der Firma Infoblox ausfallsicher innerhalb des Mandanten „Zentrale_Dienste“ bereitgestellt.

Zur Nutzung des DHCP Systems müssen in allen Netz IDs auf den Switchen der Distribution Module entsprechende IP Helper Einträge hinterlegt werden.

Die IP Helper Einträge verweisen auf eine virtuelle IP Adressen des Infoblox DHCP Appliance Systems.

IP1: 10.96.68.11

Im DHCP Server müssen alle zu versorgenden Netz IDs der Mandanten eingetragen sein. Hinzu kommen noch die relevanten Eintragungen bzgl. Gateway und DNS Server.

21.8 Administration / Konfiguration / Monitoring / Sicherung

Für den administrativen Zugang auf die Komponenten der Netzwerkinfrastruktur ist eine personifizierte Authentifizierung gegenüber einer zentralen Cisco Identity Services Engine Lösung (Cisco ISE) notwendig.

Berechtige Anwender müssen im Vorfeld der Nutzung auf dem System angelegt und entsprechend ihrer notwendigen Berechtigungen eingerichtet werden.

Bei Ausfall der zentralen Cisco ISE Lösung kann auf einen lokal eingerichteten Superuser in den Komponenten zurückgegriffen werden.

Die Konfiguration der Komponenten erfolgt überwiegend über die CLI der jeweiligen Komponente.

Das Monitoring der Komponenten der Netzwerkinfrastruktur erfolgt über das zentrale CheckMK Nagios System. Hier sind alle Komponenten aufgenommen und werden über ein Standard Monitoring-Set überwacht.

Über das CheckMK Nagios System erfolgt ebenfalls das automatische Anlegen von Aufträgen in der SAP Umgebung, z.B. in Fällen von Incidents. Hierzu ist eine Schnittstelle zum SAP Ticketsystem programmiert.

Eine Visualisierung der Netzwerkinfrastruktur hinsichtlich der Komponenten und deren Anbindungen erfolgt aktuell über die Cisco Prime Infrastrukture. Zudem ist die Cisco Prime Infrastructure für das Device- und Konfigurationsmanagement im Einsatz.

Für die tägliche Sicherung der aktuellen Konfiguration der Netzwerkdevice wird die Cisco Prime Infrastruktur verwendet. Die Sicherung der Devices wird über einen scheduled Job der Prime Infrastructure automatisch täglich durchgeführt. Hierdurch ist gewährleistet, dass ein Netzwerkdevice nach einem Ausfall mit einer gültigen Konfiguration wiederhergestellt werden kann.

21.9 Logging

Auf allen Netzwerkkomponenten ist ein Eventlogging eingeschaltet, um wichtige Systemereignisse mit zu protokolieren. Dies ist auch die Grundlage für die Überwachung durch die zentralen Managementtools von Cisco. Jedem Event im Logging ist ein Zeitstempel vorangesetzt, dies macht es aber auch nötig, dass hier eine zentrale Synchronisation der Zeit stattfindet. Hierzu gibt es einen Konfigurationseintrag. Die zentrale Zeit wird auf allen Netzwerkkomponenten von dem DHCP Server eingeholt.

21.10 WLAN Infrastruktur

21.10.1 Allgemein

Die FSG betreibt eine flächendeckende WLAN Infrastruktur in weiten Teilen der Gebäudeinfrastruktur auf dem Flughafen Campus. Die Infrastruktur basiert auf einem controllerbasierten Netzwerk des Herstellers Cisco Systems in dem neben den Steuerungscontroller unterschiedliche WLAN Access Points (APs) zum Einsatz kommen.

21.10.2 WLANs und Versorgungsbereiche

Auf der WLAN Infrastruktur werden die nachfolgenden WLANs (SSIDs) in den dargestellten Versorgungsbereichen bereitgestellt.

WLAN	T1	T2	T3	T4	P4	PWH[1]	Feuerwache	SAB[2]	Skyport
FSG Enterprise	X	X	X	X	X	X	X	X	X
Gast						X	X		X
Gast_W[3]	X[4]								
Hotspot Telekom	X	X	X	X		X	X	X	X
Hotspot Lufthansa	X[5]								
Hertz					X				
Avis					X				
ARWE (Sixt, Europcar,…)					X				

Tabelle 7: WLANs und Versorgungsbereiche

Ein weiterer Ausbau der gesamten WLAN Infrastruktur bzw. der Versorgungsbereiche der einzelnen WLANs ist in Abstimmung mit der zuständigen Fachabteilung möglich.

21.10.3 Physikalischer Aufbau

In den Versorgungsbereichen der jeweiligen Gebäude sind die WLAN APs flächendeckend installiert. Es kommen unterschiedliche Typen der Cisco WLAN Access Point Komponenten zum Einsatz.

Die WLAN Access Points werden hierbei aus den zentralen und redundanten WLAN Controllern mit ihrer entsprechenden Konfiguration versorgt. Eine lokale Konfiguration erfolgt nicht.

Als Controller kommen die Komponenten Cisco 5508 und Cisco 5520 jeweils redundant zum Einsatz. Diese sind redundant an das Core Modul angebunden.

Die ca. 230 APs sind in unterschiedlichster Ausführung und Antennentechnologien im Campus verbaut und überwiegend mit PoE auf Basis 802.1af stromseitig durch die Access Module versorgt.

Bei zukünftigen Erweiterungen / Erneuerungen sind in den Access-Modulen bzw. in den Switchen die Versorgung von 802.1at (30Watt) zu berücksichtigen. In Einzelfällen ergeben sich ggf. auch höhere Versorgungsanforderungen.

21.10.4 Logischer Aufbau

Die physischen WLAN Access Points werden in den jeweiligen Gebäuden bzw. in den Distribution Modulen in einem VLAN gesammelt und im Distribution Modul in den Mandanten FSG_AP eingespeist. Der hier entstehende Datenverkehr wird gesammelt und verschlüsselt an die zuständigen Controller gesendet. Die Verschlüsselung basiert hierbei auf den Verfahren LWAPP /

[1] PWH = Personenwohnheim (Südseite)
[2] SAB = Stuttgart Airport Busterminal
[3] Gast_W = Gästebereich Wöllhaf
[4] T1 im Bereich Konferenz und Bankett Center
[5] T1 in der Lufthansa Lounge in Ebene 4

CAPWAP. An den Controllern wird der Verkehr in Bezug auf den entsprechenden Mandanten / Kunden unverschlüsselt weiter transportiert.

Je nach Anforderungen und notwendiger Kommunikationsbeziehungen werden die logischen Verbindungen, WLAN bezogen, über das Firewall Modul in den Rechenzentren weiteren Mandanten / Kundennetzen zugeführt.

Nachfolgendes Übersichtsbild zeigt beispielhaft den logischen Aufbau und die Anbindungen.

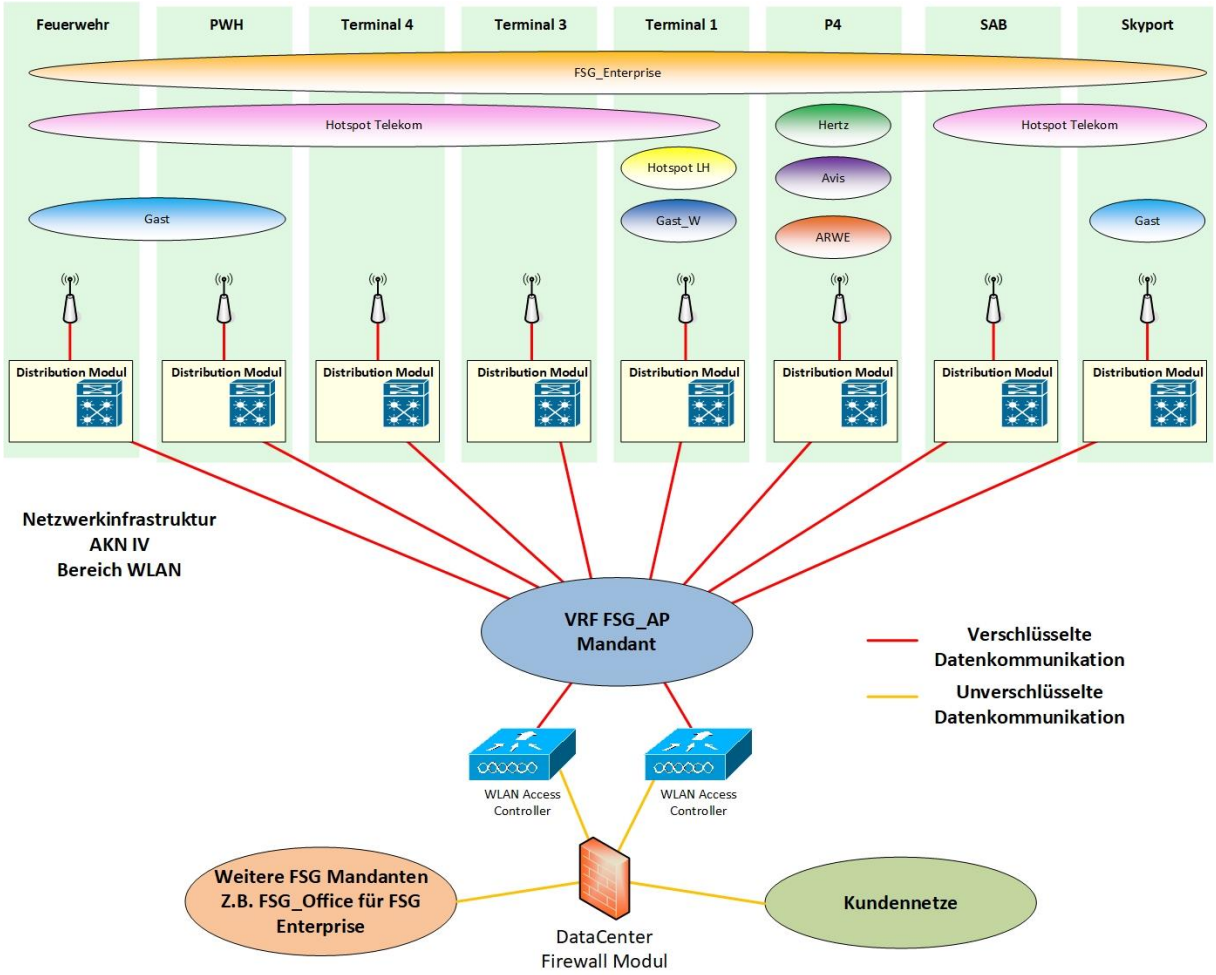

Abbildung 12 Übersichtsbild logischer Aufbau der WLAN Infrastruktur

21.10.5 Authentifizierung und Security in den WLANs

Die WLANs aus **Fehler! Verweisquelle konnte nicht gefunden werden.** werden bis auf den Telekom Hotspot mit einer Verschlüsselung abgesichert. Hierbei wird überwiegend WPA2 verschlüsselt.

Im FSG Enterprise WLAN ist zur Absicherung des Zuganges zum WLAN das Protokoll 802.1x im Einsatz.

Im Bereich der Authentifizierung als Zugang zu den WLANs werden unterschiedliche Methoden eingesetzt. Diese werden nachfolgend kurz erläutert.

FSG_Enterprise:

Hierbei wird eine anwenderbezogene Authentifizierung über das Active Directory der FSG eingesetzt. In Zukunft wird hier auf eine zertifikatsbasierte Methode über die FSG eigene PKI Infrastruktur umgestellt. Die Anwender müssen sich entsprechend der Methode gegenüber dem Active Directory authentifizieren und erhalten danach den Zugang zum FSG_Enterprise WLAN. Dieses ist mit den

Standard FSG Services und dem FSG_Office Mandanten verbunden. Hierdurch sind alle FSG bezogenen Zugriffsrichtlinien z.B. hinsichtlich Internet / Proxy Einstellungen verfügbar und werden angewendet.

Gast und Gast_W:

Die notwendigen Zugangsdaten zu den Gast WLAN Bereichen werden durch das Kundencenter (Tel. 3000), den Empfang im Skyport oder am Empfangsbereich T1 KBC (für Gast_W) ausgegeben.

Nach Anmeldung an einer entsprechenden FSG Zugangsseite im Browser des Rechners erhalten die Gäste Zugriff auf das Internet. Die Absicherung bzw. Verifizierung des Gast-Zuganges erfolgt hierbei über die CISCO ISE der FSG.

Telekom Hotspot und Lufthansa Hotspot:

An die beiden Hotspots können sich alle Anwender für 1 Stunde kostenlos verbinden und auf das Internet zugreifen. Vertragskunden der Telekom erhalten entsprechenden einen 24 Stunden Zugriff.

Autovermieter (AVIS, Hertz, AWE):

Der Zugriff auf diese WLANs basiert auf den MAC Adressen der Teilnehmer. Diese werden durch die FSG auf den Controllern eingetragen und gepflegt. Entsprechend eingetragene MAC Adressen erhalten somit den Zugang zu dem entsprechenden WLAN.

Zur Eintragung und Pflege nennen die Firmen über einen Auftrag an das Kundencenter die MAC Adresse des entsprechenden Endgerätes welches aufgenommen oder gelöscht werden soll.

21.10.6 Adressvergabe in den WLANs

Die Adressvergabe der IP Adressen erfolgt entweder durch die zentralen DHCP Dienste der FSG oder durch kunden- bzw. providereigene Verfahren.

21.10.7 Management / Heat MAP

Wie im Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** dargestellt, sind alle Komponenten in das Cisco Prime Management integriert. Die WLAN Access Points werden hierbei automatisch im System aufgenommen. Zur genauen Visualisierung der Versorgungsbereiche bzw. des Standortes werden die APs nach der Aufnahme manuell auf einer MAP basierend auf den jeweiligen Gebäudegrundrissen positioniert.

Durch die Positionierung und der Darstellung in der MAP ist im Management relativ aktuell eine Heatmap der entsprechenden Ausleuchtung und Belastung der WLAN Infrastruktur darstellbar.

21.11 Firewall / Security

Aus Sicht der Netzwerkmodularisierung sind im Bereich Firewall / Security bei der FSG derzeit zwei Firewall Module im Einsatz

- DataCenter Firewall Modul
- Edge Firewall Modul

Das DataCenter Firewall Modul trennt den internen Verkehr zwischen den Mandanatenstrukturen innerhalb des AKNs und das Edge Firewall Modul ist grundsätzlich für die externen Kommunikationsverbindungen so wie Verbindungen in die DMZ von und zu den AKN Mandanten verantwortlich.

21.11.1 DataCenter Firewall Modul

Im DataCenter Firewall Modul ist derzeit eine redundante Lösung, basierend auf den Komponenten Firepower 4115 Security Appliance von Cisco Systems, in den beiden Rechenzentren verbaut und im Einsatz.

Der Aufbau besteht aus einem aktiv/aktiv Cluster, welcher auf die zwei Rechenzentren RZ1 und RZ2 verteilt ist. Beim Ausfall eines Teilnehmers schwenken die Instanzen automatisch auf den noch aktiven Host, so dass die Funktion nicht beeinträchtigt wird. Der Firewall Cluster ist die Plattform für virtuelle Firewall Instanzen, durch die die Trennung von einzelnen Systembereichen realisiert wird.

Regelwerk der Datacenter Firewall:

Das Regelwerk der Datacenter Firewall wird derzeit anhand der verwendeten IP Adressen der Kommunikationsbeziehungen aufgebaut. Aus diesen Gründen sind die verwendeten Regeln Geräte und IP spezifisch und somit dürfen sich die zugehörigen IP Adressen der Kommunikationspartner nicht ändern. Für Regelwerke können sowohl IP-Adressen als auch FQDN verwendet werden.

Zur Eingabe von notwendigen Kommunikationsbeziehungen für Systeme, Anwendern und Anwendungen über den Firewall Kern hinweg ist das entsprechende Formblatt von FB4 zu verwenden und entsprechend auszufüllen. Hierin sind die notwendigen Angaben und Vorgaben für die gewünschte Kommunikationsbeziehung einzutragen und FB4 zur Erstellung vorzulegen.

Im Regelwerk wird sowohl auf Ports als auch auf Applikationsebene gefiltert. Des Weiteren werden die Verbindungen auf Malware überprüft und mit einem Intrusion Prevention System (IPS) überwacht.

21.11.2 Edge Firewall Modul

21.11.2.1 Allgemein

Die FSG betreibt im Edge Firewall Modul einen redundanten Firewall Kern an dem die folgenden Funktionsbereiche / -übergänge angekoppelt sind:

- AKN Anbindung (Inside) zu den Mandanten
- DMZ Umgebung
- VPN Zugangsportal
- Provideranbindung

In den Kopplungsebenen der einzelnen Funktionsbereichen bzw. -übergängen werden Cisco 3850 Gigabit Switche zur Anbindung eingesetzt.

In den nachfolgenden Kapiteln wird die Firewall Stufe und die einzelnen angekoppelten Bereiche näher beschrieben und dargestellt.

21.11.2.2 Kopplungsebenen

Zur Unterscheidung der jeweiligen Kopplungsebene werden bei der FSG folgende Bezeichnungen verwendet. (nachfolgende Sichtweise Inside → Outside → Internet)

- DMZ – Kopplungsebene zwischen der AKN (Inside) Netzwerk mit allen Mandanten und dem Firewall Kern
- Outside – Kopplungsebene zwischen Firewall Kern und Routerstufe Outside

- Internet – Kopplungsebene zwischen Router Internet und den Provider Routern

Zusätzlich zu den Switching Kopplungsebenen wird zwischen Outside und Internet noch ein Layer 3 Übergang in Form einer Routing Kopplungsebene mit der Bezeichnung „Router Internet“ betrieben. Hier werden zwei Cisco 8200er Router für die Anbindung zum Provider Telekom eingesetzt. Für die zukünftige Multiprovider Anbindung werden zwei Router vom Typ Cisco ASR1001 verwendet.

In dieser Layer 3 Stufe erfolgt die Umsetzung zwischen den offiziellen IP Adressbereichen der FSG und der internen IP Adressierung.

Für die Redundanz und Ausfallsicherheit des Kommunikationsverkehrs wird in dieser Kopplungsebene HSRP für die Gateway Adressen in den Outside Netzen und in den Internet Netzen eingesetzt. Bei der zukünftigen Multiprovider Anbindung wird für die Providerübergreifende Ausfallsicherheit im BGP Routing die Übergabe der Routen realisiert.

Die 3 Switching Kopplungsebenen sind jeweils mit 2 * Cisco 3850 Switchen im RZ2 und 1 * Cisco 3850 Switch im RZ 1 ausgeführt. Hierbei sind die Switche zwischen den RZs mit einem 2 Port Etherchannel und innerhalb des RZ 2 einfach miteinander verbunden. Auf logischer Ebene stehen auf allen 3 Switchen die gleichen VLANs für die Anbindung der Komponenten zur Verfügung.

Nachfolgendes Übersichtsbild zeigt das Edge Firewall Modul

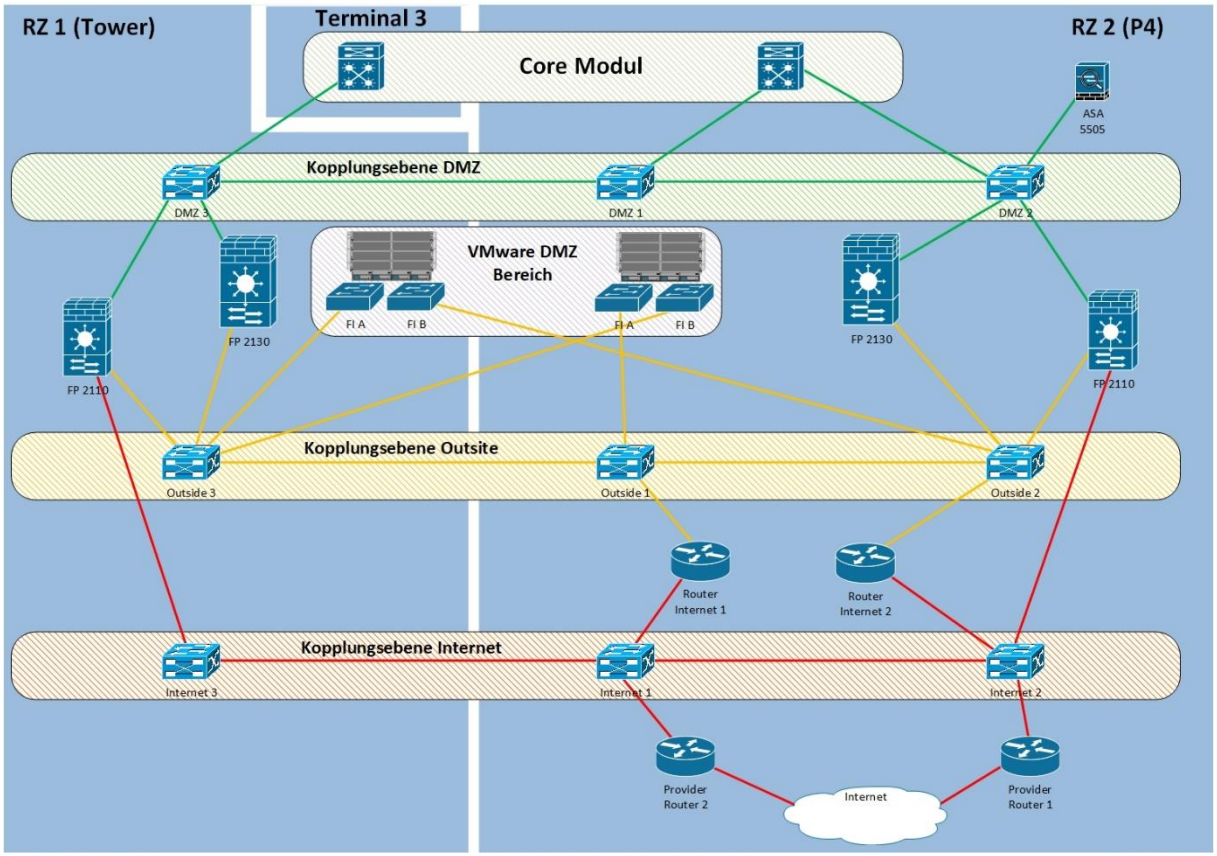

Abbildung 13 Übersichtsbild Aufbau Edge Firewall Modul

21.11.2.3 Edge Firewall

Als Edge Firewall ist eine redundante Firewall Cisco FirePower 2130 des Herstellers Cisco Systems im Einsatz. Diese wird im Active / Standby Modus betrieben, wobei der aktive Part im im RZ 1 und die Standby Hardware im RZ 2 eingebaut ist.

Alle Verbindungen von und zur FirePower sind mittels Ethernet 1Gbit ausgeführt. Jede Firepower 2130 ist hierbei mit 4 * Gbit an die Switche der Outside Kopplungsebene und mit 2 * Gbit an die Switche der DMZ Kopplungsebene angebunden.

Regelwerk der Edge Firewall:

Das Regelwerk des Firewall Kerns wird derzeit anhand der verwendeten IP Adressen der Kommunikationsbeziehungen aufgebaut. Aus diesen Gründen sind die verwendeten Regeln Geräte und IP spezifisch und somit dürfen sich die zugehörigen IP Adressen der Kommunikationspartner nicht ändern. Für Regelwerke können sowohl IP-Adressen als auch FQDN verwendet werden.

Zur Eingabe von notwendigen Kommunikationsbeziehungen für Systeme, Anwendern und Anwendungen über den Firewall Kern hinweg ist das entsprechende Formblatt von FB4 zu verwenden und entsprechend auszufüllen. Hierin sind die notwendigen Angaben und Vorgaben für die gewünschte Kommunikationsbeziehung einzutragen und FB4 zur Erstellung vorzulegen.

Im Regelwerk wird sowohl auf Ports als auch auf Applikationsebene gefiltert. Des Weiteren werden die Verbindungen auf Malware überprüft und mit einem Intrusion Prevention System (IPS) überwacht.

21.11.2.3.1 AKN Anbindung (Inside)

Die Anbindung an das AKN (Inside) erfolgt über die Kopplungsebene „DMZ“ zwischen dem AKN Core Modul mit den Cisco 9600 Switchen im VSS Verbund und dem Firewall Kern mit den Cisco FirePower 2130 Firewall Komponenten.

Hierüber werden alle Kommunikationsbeziehungen gefahren, die aus dem FSG_Office Mandanten in Richtung des Edge Firewall Moduls notwendig sind. Hierunter fallen alle direkten Anforderungen aus dem Mandanten als auch Anforderungen aus weiteren AKN Mandanten, die generell oder wegen notwendiger Anforderungen in den Kommunikationsbeziehungen mittels des DataCenter Firewall Moduls mit dem FSG_Office Mandanten verbunden sind.

Eventuelle direkte Verbindungen aus AKN Mandanten in Richtung Internet oder DMZ Diensten werden über eine direkte Verbindung des DataCenter Firewall Moduls auf die Outside Kopplungsebene in das Modul eingespeißt.

21.11.2.3.2 DMZ Umgebung

Die DMZ Umgebung wird duch einen separatierten redundanten VMware Cluster über die beiden Rechenzentren RZ 1 und RZ 2 bereitgestellt.

Hierzu sind entsprechende vom produktiven VMware Cluster unabhängige VMware Hosts in der DataCenter Computing Umgebung der FSG in den jeweiligen DataCenter Bereichen der Rechenzentren im Einsatz. Diese Computing Ressourcen werden jeweils in den RZs durch ein Cisco UCS System vom Hersteller Cisco Systems bereitgestellt. Für die Anbindung der Computing Ressourcen werden in der UCS Systemumgebung sogenannte Fabric Interconnect Komponenten verwendet.

Die physische Netzwerkanbindung des VMware DMZ Clusters bzw. seiner Fabric Interconnect Komponenten erfolgt mittels entsprechender Channelverbindungen zwischen dem Fabric Interconnect und den Switchen in der Outside Kopplungebene.

Insgesamt sind folgende Verbindungen konfiguriert.

- RZ1-FI-A → RZ1-Outside 3 mit 2 * 1Gbit
- RZ1-FI-B → RZ2-Outside 2 mit 2 * 1Gbit
- RZ2-FI-A → RZ2-Outside 1 mit 2 * 1Gbit
- RZ2-FI-B → RZ1-Outside 3 mit 2 * 1Gbit

Innerhalb der DMZ Umgebung sind die zu verwendenden Netzwerkbereiche für Applikationen / Systeme oder Appliances entsprechend fachbereichsbezogen aufgebaut.

Für jeden Fachbereich sind folgende Netzwerkbereiche vorbereitet:

- Ein Class C Netzwerk welches in weitere 8 Subnetze mittels eines /27 Subnettings unterteilt ist.
- In jedes Subnetz können nach Abstimmung oder Vorstellungen der Fachbereiche bestimmte Funktionsbereiche aufgenommen bzw. integriert werden.

In der Übergangszeit sind derzeit die bestehenden Applikationen / Systeme / Appliances in zwei weiteren Class C Netzwerken integriert. Eine Migration bzw. eine Umstellung erfolgt hier im Zuge von Erneuerungs- bzw. Migrationsprojekten der jeweiligen Funktionseinheiten.

21.11.2.3.3 VPN Zugangsportal

Als Teilbereich der DMZ oder auch eigenständig kann das VPN Zugangsportal der FSG bezeichnet werden. Über das Portal erfolgen bzw. terminieren entsprechende VPN Site-to-Site Verbindungen und Remote Access Verbindungen.

Im VPN Zugangsportal sind folgende Komponenten im Einsatz:

- Cisco FirePower 2110

Im Umfeld des VPN Zugangsportals ist eine redundante Firewall Cisco FirePower 2110 des Herstellers Cisco Systems im Einsatz. Die FirePower wird im Active / Standby Modus betrieben, wobei der aktive Part im im RZ 1 und die Standby Hardware im RZ 2 eingebaut ist.

Die Komponenten / Systeme sind an die entsprechenden Switche der Kopplungsebenen angeschlossen. Alle Verbindungen sind mittels Ethernet 1Gbit ausgeführt. Hierbei bestehen folgende Verbindungen

- Firepower 2110 RZ 1 und RZ 2
  - ✈ Anbindung an Kopplungsebene DMZ
  - ✈ Anbindung an die Kopplungsebene Outside als Zugang für die VPN Tunnel und die RA Verbindungen
  - ✈ Anbindung an die Kopplungsebene Internet als Zugang für die Bereitstellung von offiziellen IP Adressen im Rahmen des VPN Portals

Über das VPN Zugangsportal wird der Corperate Data Access (CDA) zu den Providern Vodafone und Telekom bereitgestellt und betrieben. Für den Beitrieb dieser CDA Verbindungen ist die Bereitstellung des Dienstes über offizielle IP Adressen notwendig, die über die dargestellte Anbindung an die Kopplungsebene Internet realisiert wird.

Weiterhin terminieren am Portal die entsprechenden Remote Access (RA) Verbindungen, die als Vorgabe der FSG, durch entsprechende Cisco Anyconnect VPN Client Software aufgebaut werden können.

Die Bereitstellung einer VPN Site-to-Site Verbindung oder eines Remote Access Zuganges erfolgt über das Auftragsmanagement der FSG oder über das Firewall Formblatt von FB4. Eine Integration in ein entsprechendes WEB Formular ist in Vorbereitung.

Die Freischaltung des Zuganges bzw. der Aufbau des VPN Tunnels im Cisco AnyConnect VPn Client erfolgt für Interne und Externe Mitarbeiten auf unterschiedliche Art und Weise.

- Interne Anwender erhalten Zugriff über das Ihnen zugehörige PKI Zertifikat
- Externe Anwender müssen Ihren Client über Benutzername / Passwort authentisieren. Die Zugangsdaten werden über die Active Directory (AD) von FB3 bereitgestellt. Eine zweite Authentifizierung (Multifaktor) wird über das Webportal Microsoft Authenticator realisiert. Hiermit kann der zweite Faktor über eine App, einen Rückruf oder eine SMS bestätigt werden.

Die Bereitstellung des Cisco AnyConnect VPN Client erfolgt im Falle von externen Mitarbeitern über E-Mail. Im Falle von internen Mitarbeitern wird der Cisco Secure Client über die Softwareverteilung installiert. Alle internen Mitarbeiter erhalten automatisch mit der Beauftragung eines AD-User einen Standard FSG VPN Zugang. Werden erweiterte Berechtigungen/Abteilungsberechtigungen benötigt, müssen diese begründet und über das Servicecenter beauftragt sowie mit einem entsprechenden Change genehmigt werden.

Die Einführung einer 2 Faktoren Authentifizierung für die Remote Verbindungen ist in Planung. Dies betrifft dann die folgenden Verbindungsarten und Applikationen:

- Nachrichtenmanager
- PasswortStore
- AD Priviligierte Accounts
- E-Mail mit Vertraulichkeitsstufe
- Sharepoint von Extern
- etc.

21.11.2.3.4 Provideranbindung

Auf Seiten der Provideranbindung in Richtung Internet steht zurzeit eine redundante Anbindung im RZ 2 über den Provider Telekom zur Verfügung.

Die Anbindung erfolgt über ein Routerpärchen der Telekom mit einer synchronen Bandbreitenauslegung der beiden Verbindungsleitungen.

Die primären Anbindung ist mit 150Mbit und die sekundäre (Backup) Anbindung ebenfalls mit 35Mbit ausgelegt. Beide Anbindungen können aktiv genutzt werden. Von Seiten des Providers wird in der Konfiguration der Router ein Ausfall einer Verbindung erkannt und es erfolgt eine Umschaltung des gesamten Verkehrs auf die verbleibende Verbindung. Im Normalbetrieb erfolgt eine Verteilung der Last mittels einer Verkehrsflusssteuerung auf Basis bestimmter Adressen zw. Adressbereichen.

Die Router der Telekom sind an die Kopplungsebene Internet mit jeweils 1 Gbit Anschluss angebunden. Hierbei werden die beiden Router mit ihrem Anschluss auf die Internetswitche im RZ 1 und RZ 2 verteilt. Hierdurch ist somit auch eine Komponentenredundanz in der Kopplungsebene realisiert.

In einem zukünftigen Projekt soll die bestehende einfache Providerauswahl in eine Multiprovideranbindung geändert werden. Im Zuge dieser Realisierung erfolgt dann auch eine Verteilung der Provider auf die beiden Rechenzentren RZ 1 und RZ 2 und eine homogene / synchrone Auslegung der Anbindungsbandbreite.

21.11.3 DNS Protection

Mit dem Cloud basierten System Cisco Umbrella wird bereits die DNS Anfrage von Systemen überwacht und die Namensauflösung zu als gefährdend eingestuften Links blockiert. Zusätzlich kann auch überprüft werden, auf welche SaaS (Software as a Service) die Nutzer zugreifen. Mit dem inkludierten CloudLock (auch Cloud Access Security Broker genannt) lassen sich beispielsweise unangemessene Apps sperren. Die Lösung Umbrella leitet Anfragen transparent um und zeigt anstelle der Zielseite einen vordefinierten Hinweis, dass die Verbindung geblockt wurde.

21.12 Netzwerkmanagement

21.12.1 Funktionsbereiche

Die vielfältigen IT-Managementaufgaben in einem unternehmensweiten Netzwerk erfordern die Einteilung der Management-Anforderungen in Funktionsbereiche. 1989 veröffentlichte die International Standard Organisation (ISO) 5 Funktionsbereiche die noch heute ihre Gültigkeit besitzen. Die festgelegten Funktionsbereiche werden entsprechend ihrer fünf Anfangsbuchstaben in englischsprachiger Literatur oftmals auch als FCAPS bezeichnet. Die Unterteilung in die folgenden fünf Funktionsbereiche wurde wie folgt durchgeführt:

- **(F) Fehler- und Problem Management:** Erkennung, Lokalisierung und Behebung von Fehlern, Erstellung von Reports für die Anwender und IT-Verantwortlichen, Erstellung von Fehler-Historien zur Feststellung von Trends
- **(C) Configurations Management:** Steuern, Setzen und Sammeln der Parameter und Daten der Management-Objekte (IT-Komponenten)
- **(A) Accounting Management:** Zuordnung der Nutzung von Netzressourcen zu den Anwendern oder Anwendergruppen und/oder Änderungsplanung bei den Kapazitätsanforderungen
- **(P) Performance Management:** Ermittlung von Daten zur Analyse, zur Optimierung der Ressourcen sowie zur Kapazitätsplanung. Nachweis über die Einhaltung von Service Level Agreements (SLAs)
- **(S) Security Management:** Überwachung und Überprüfung der Einhaltung der Sicherheitsvorgaben, Verwaltung und Verteilung von Kennwörtern und weiterer Authentifizierungs- und Autorisierungsinformationen

Die Netzwerkmanagementlösung in der FSG setzt sich aus mehreren Netzwerkmanagementprodukten zusammen. Die zum Einsatz kommenden SW-Produkte

- Check MK
- Cisco Prime
- Splunk
- PRTG

decken unterschiedliche Funktionsbereich des Netzwerkmanagements ab.

Die einzelnen SW-Produkte und ihre Einsatzgebiete werden in den folgenden Kapiteln näher erläutert.

21.12.2 CheckMK (Nagios)

CheckMK wird als zentrales Fehler- und Performance Management System bei der FSG eingesetzt.

Das Produkt basiert ursprünglich auf dem Produkt Nagios und erweitert dies um weitere Komponenten.

Das Monitoring der Netzwerkinfrastrukturkomponenten erfolgt über ein Standard Monitoring- Set indem folgende Parameter überwacht werden:

- Systemstatus (online/offline)
- Status von Redundanzen
- Status von Ports (nur ausgewählte Devices)
- Traffic
- Status von CPU, Modulen, Lüftern, Netzteilen

Weiterhin stellt das Produkt die zentrale Schnittstellte zum SAP Troubleticket-System zur Verfügung. Über diese Anbindung werden in Abhängigkeit der Kritikalität der Events (Major) automatisch Troubletickets generiert bzw. bei entsprechenden Events (Clear) auch die automatische Schließung von Troubletickets veranlasst.

Folgende Funktionen werden darüber abgedeckt:

- Fehler- und Problemmanagement aller Netzwerk- und IT-Komponenten
  - Monitoring Netzwerk- und IT-Komponenten
  - Zentrale Ereigniskonsole
  - Graphische Business View
- Performance Management

21.12.3 Cisco Prime Infrastructure

Cisco Prime Infrastructure wird für das LAN-Management der kabelgebundenen und drahtlosen Netzwerkkomponenten des Hersteller Cisco eingesetzt. Die Softwarelösung ist die Managementplattform für FB4. Alle Netzwerkkomponenten sind in das Cisco Prime Management integriert.

Die Netzwerkkomponenten schicken beim Auftritt eines Ereignisses eine unaufgeforderte Nachricht (SNMP Trap) an die Softwarelösung über eine definierte IP-Adresse. Die Meldungen werden anschließend entsprechend eines vordefinierten Regelwerkes behandelt und auf einer Alarmkonsole dargestellt. Weiterhin werden Syslog Meldungen der Netzwerkkomponenten an die Softwarelösung weitergeleitet.

Alle aus der Verarbeitung der SNMP-Traps resultierenden Events werden von der Softwarelösung an die Software CheckMK weitergeleitet.

Neben der zentralen Verarbeitung und Annahme von SNMP-Traps wird auch ein hierarchisches Netzwerk-Discovery und eine grafische Darstellung der MPLS-Topologien durchgeführt. Hierfür polled die Software mittels SNMP aktiv die Netzwerkkomponenten und erfasst so Grundinformationen bzgl. Hardware, Netzwerkkonfiguration und Erreichbarkeit der Systeme.

Zur genauen Visualisierung der Versorgungsbereiche bzw. des Standortes der WLAN_Infrastruktur werden die AccessPoints, nachdem sie automatisch erkannt wurden, manuell auf einer MAP basierend auf den jeweiligen Gebäudegrundrissen positioniert. Durch die Platzierung in der MAP wird die entsprechende Ausleuchtung in Form einer sog. Heatmap der WLAN Infrastruktur dargestellt.

Für die tägliche Sicherung der aktuellen Konfiguration der Netzwerkdevice wird die Cisco Prime Infrastruktur verwendet. Die Sicherung der Devices wird über einen scheduled Job der Prime Infrastructure automatisch täglich durchgeführt. Hierdurch ist gewährleistet, dass die Netzwerkkomponenten nach einem Ausfall mit einer gültigen Konfiguration wiederhergestellt werden können.

Folgende Funktionen werden darüber abgedeckt:

- Configurations Management
  - Device Inventory (Geräteverwaltung)
  - Compliance (Überwachung von Konfigurtationsvorgaben)
  - Rollout und Archivierung von Konfigurationen
  - Topologiedarstellung Netzwerk
  - Heatmap für WLAN-Controller
- Fehler- und Problem Management für die Netzwerkspezialisten FB4
  - Polling der Netzwerkkomponenten,
  - Trapreceiver,
  - Syslogserver

21.12.4 Splunk

Mittels Splunk Enterprise werden die Logdaten der Cisco Ironport Web Security Appliances, der Edge und Datacenter Firewalls und der Cisco Identity Solution Engines zentral protokolliert. Zielsetzung hierbei ist es, dass bei Verdacht auf missbräuchliche Nutzung der Internet- bzw. WLAN-Umgebung eine Protokollauswertung durchgeführt werden kann.

21.12.5 PRTG

PRTG wird als Performance Monitoring Tool für spezielle Komponenten eingesetzt. Mit Hilfe von PRTG wird die Auslastung der Internetanschlüsse überwacht. PRTG liest per SNMP-Protokoll die Interfaceauslastung der Router aus und stellt diese grafisch dar.

21.13 Telefonie

21.13.1 VoIP System

Die Voice over IP Telefonanlage wird verwendet um Standard Büro Telefone miteinander zu vernetzen. Jedes Telefon wird an einen Standard AKN Anschluss angeschlossen und kommuniziert über ein abgetrenntes VLAN Mit den VoIP Servern und den anderen Telefonen.

Das VoIP System besteht aus zwei virtuellen Servern: SRVVOIPOSV1 und SRVVOIPOSV2. Eine Erweiterung der VoIP Anlage sind die Softphones und Desktopintegrationen. Mithilfe eines Softphones kann direkt von PC aus ohne ein Hardwaregerät telefoniert werden. Hierzu wird eine paketierte Software von FB3 verteilt. Die Desktopintegration hilft dabei einen Überblick über verpasste Anrufe zu erhalten. Sie kann als eine Art Fernbedienung angesehen werden. Zum Telefonieren wird hierbei ein Hardwaretelefon benötigt.

Um diese Funktionen zur Verfügung zu stellen sind die folgenden virtuellen Server im Einsatz:

SRVVOIPDLS	Zur Einrichtung und Konfiguration der Hardware Telefonie Endgeräten
SRVVOIPUC	Backend für die Desktopintegration und das Softphone
SRVVOIPUCFE	Frontend für die Desktopintegration und das Softphone
SRVVOIPFS	Steht in der DMZ um die Verbindung zur Smartphoneapp her zu stellen

Hinzu kommt ein Server, um die Anrufbeantworter der FSG zu konfigurieren und einzurichten. Ein Teilnehmer kann nach Einrichten eines Kontos sein Telefon auf die -9403 umleiten und hat dadurch einen Sprachspeicher zur Verfügung. Der dazugehörige Server ist ebenfalls virtuell: SRVVOIPX

21.13.2 Zweidrahttelefonie

Die Zweidrahttelefonie wird über sieben einzelne Knotenpunkte gelöst. Von dort aus werden die Drähte bis zum Endgerät durchgeschalten. Die Zweidrahttelefonie wird für externe Firmen verwendet sowie Notfalltelefone oder in kritischen Bereichen. Da die Telefone direkt über die Anlage mit Strom versorgt werden und nicht über das AKN Netzwerk verbunden sind ist die Zweidrahttechnologie sehr ausfallsicher. Die Zweidrahtanlage wird auch verwendet, um Fax für MFP Geräte bereit zu stellen und um Analogtelefone anzuschließen, wie beispielsweise wetterfeste Außengeräte. Die Vernetzung der einzelnen Knotenpunkte erfolgt über eine Glasfaserleitung direkt von Anlage zu Anlage. Sollte durch einen Defekt diese Leitung unterbrochen sein wird die Backupverbindung über das Standard FSG Kupfer Netzwerk verwendet. Zusätzlich zu den sieben physikalischen Servern kommt ein virtueller Server (SRVVOIP4M) der als zentrale Managementplattform dient. Die Knotenpunkte sind an folgenden Standorten: P4/Rechenzentrum, Terminal 1, Terminal 3, OPS Gebäude, Feuerwache und auf der Südseite.

21.13.3 Callcenter / Infocenter

Das Callcenter des Flughafens übernimmt alle Anrufe der Hauptrufnummer +497119480. Verteilt werden sie durch das sogenannte Consierge. Hierzu gehören einige virtuelle Server welche direkt mit der Zweidrahttelefonanlage im Terminal 3 kommunizieren. Das Consierge übernimmt sowohl das Managen der Warteschlangen, die angemeldeten Agenten, die gleichmäßige Verteilung der Anrufe

auf die angemeldeten Agenten und das Routing der Anrufe welches je nach Tageszeit und Anrufsziel unterschiedlich sein kann.

Folgende Server sind dafür im Einsatz:

SRVVOIPCC02	Backend für das Consierge System
SRVVOIPCON02	Stellt die Consiergesoftware für die Anwender bereit
SRVVOIPCMS02	
SRVVOIPCT01	Datenbankserver für das Consiergesystem
SRVVOIPMD01	Telefonbuch für die Vermittlungsstellen

Zusätzlich kommen zwei Mediaserver hinzu, welche die Musikdateien für Warteschlangen beinhalten.