Charta Products

Skapa ett säkert nät

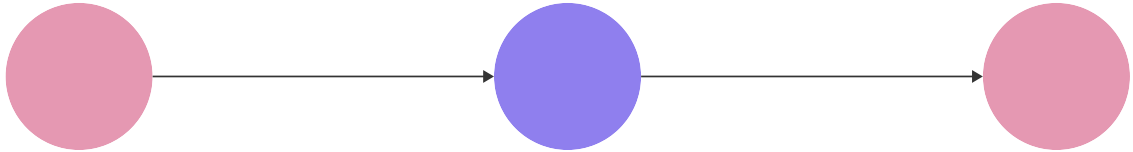
2 april 2025

Allen Camille Muco
Hugo Polstam
Isac Safarov
Nicholas John Stevens
Sebastian Ekedahl

Agenda

1. Hotbildsanalys
2. Översikt av nätverksdesign
3. Säkerhetsåtgärder och konfiguration
4. Utrustnings- och programvarulista
5. Riskbedömning och åtgärder

Uppgift



Varför?

Charta Products AB behöver modernisera och säkra sitt nätverk. Därför bygger de en helt ny nätverksinfrastruktur.

Vad har vi gjort?

Vi har analyserat hotbilden, identifierat sårbarheter och tagit fram en säker och skalbar nätverkslösning.

Vad är vår strategi?

Att skapa ett segmenterat och säkert nät med VPN, brandväggar och stark autentisering – både för interna och externa användare.

1. Hotbildsanalys

Risknivå: Hög

A. Ransomware och Malware

Företaget har tidigare drabbats av ransomware som orsakat driftstopp och ekonomiska förluster.

Risknivå: Medelhög

B. Phishing och Social Engineering

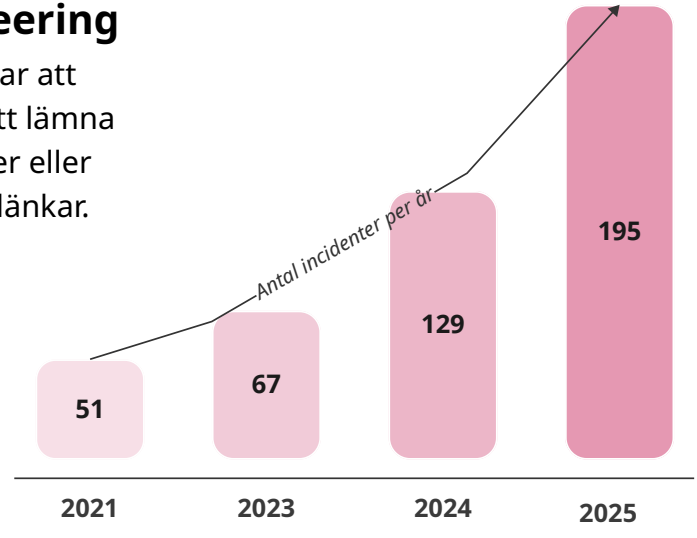
Anställda riskerar att luras via mejl till att lämna ifrån sig uppgifter eller klicka på farliga länkar.

Risknivå: Medelhög–Hög

C. Osäkert Wi-Fi och MITM

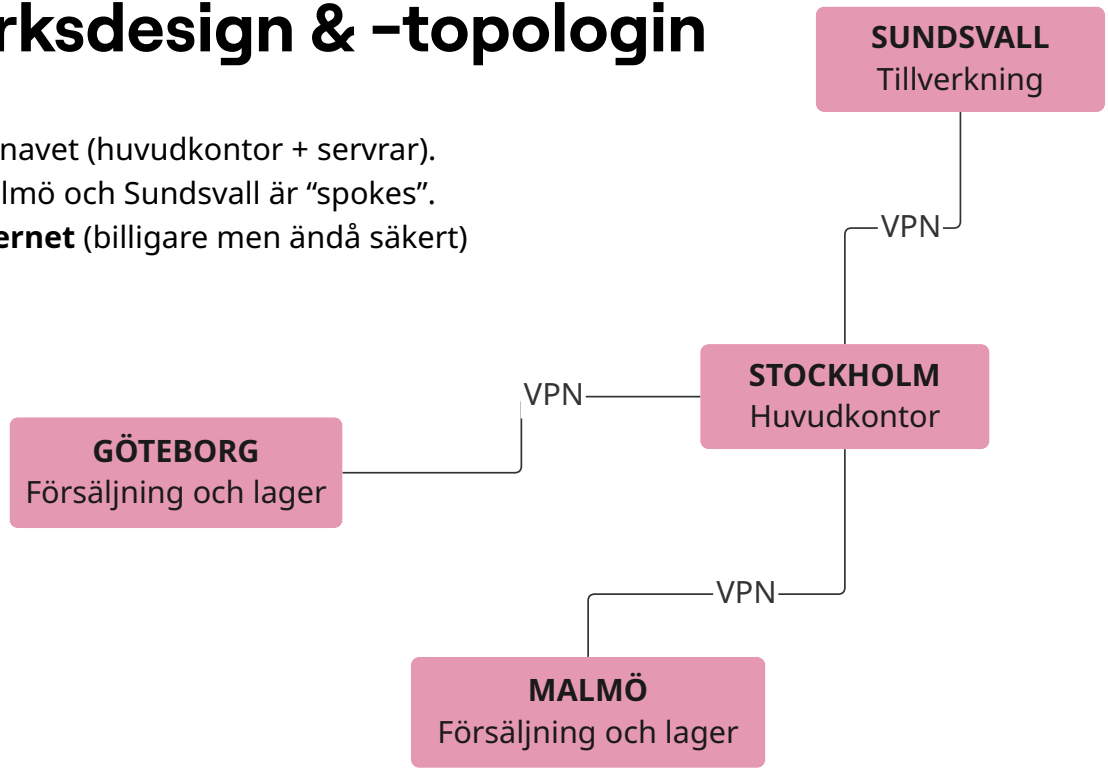
Osäkert Wi-Fi och svagt konfigurerad VPN kan utnyttjas för attacker.

Vi använder detta som ett illustrativt exempel baserat på Chartas situation.



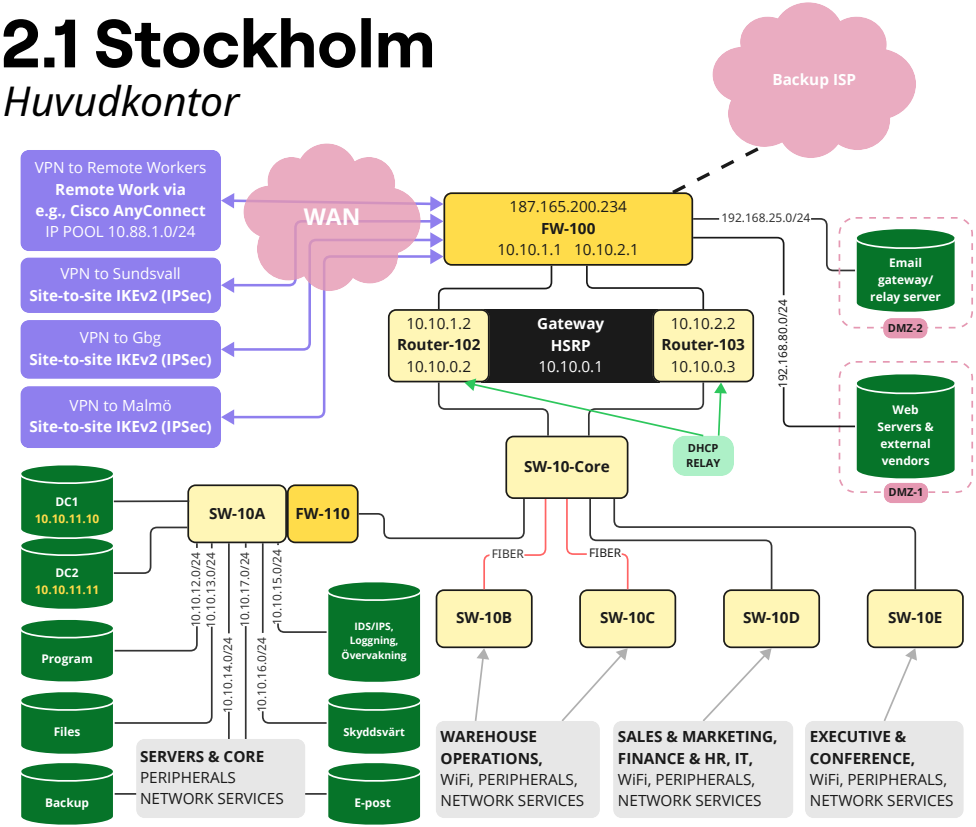
2. Nätverksdesign & -topologin

- Stockholm är navet (huvudkontor + servrar).
- Göteborg, Malmö och Sundsvall är “spokes”.
- **VPN över internet** (billigare men ändå säkert)



2.1 Stockholm

Huvudkontor



STOCKHOLM: VLAN

DMZs
- **80 DMZ-1** Web server / services
- **25 DMZ-2** Email gateway / relay

SERVERS & CORE
- **111** Domain controllers
- **112** Software / internal services
- **113** Static file storage
- **114** Backup infrastructure
- **115** IDS/IPS, övervakning, logging
- **116** Confidential Data
- **117** Backend mail / internal flow

WAREHOUSE OPERATIONS
- **121** Workstations/terminals
- **122** Wireless devices/scanners

SALES & MARKETING
- **131** Workstations
- **132** VoIP

FINANCE & HR
- **141** Finance-Data: workstations
- **142** HR-Data: workstations

EXECUTIVE & CONFERENCE
- **151** Executive offices
- **152** Conference rooms

IT
- **161** IT-Admin: IT workstations

WiFi
- **171** Employee-Wireless
- **172** Guest-Wireless

PERIPHERALS
- **190** Printers
- **191** Embedded Devices (IoT)
- **196** Physical Security Systems

NETWORK SERVICES
- **197** Backup/disaster recovery
- **198** Logging and monitoring
- **199** Network-wide management

STOCKHOLM: SUBNETTING

DMZ
- **192.168.25.0/24** DMZ1-Webb
- **192.168.80.0/24** DMZ2-E-post

STOCKHOLM LAN
- **10.10.0.0/16**

SERVERS
- **10.10.11-17.0/24**

WAREHOUSE
- **10.10.21-22.0/24**

SALES
- **10.10.31-32.0/24**

FINANCE & HR
- **10.10.41-42.0/24**

EXECUTIVE
- **10.10.51-52.0/24**

IT-DEPARTMENT
- **10.10.61.0/24**

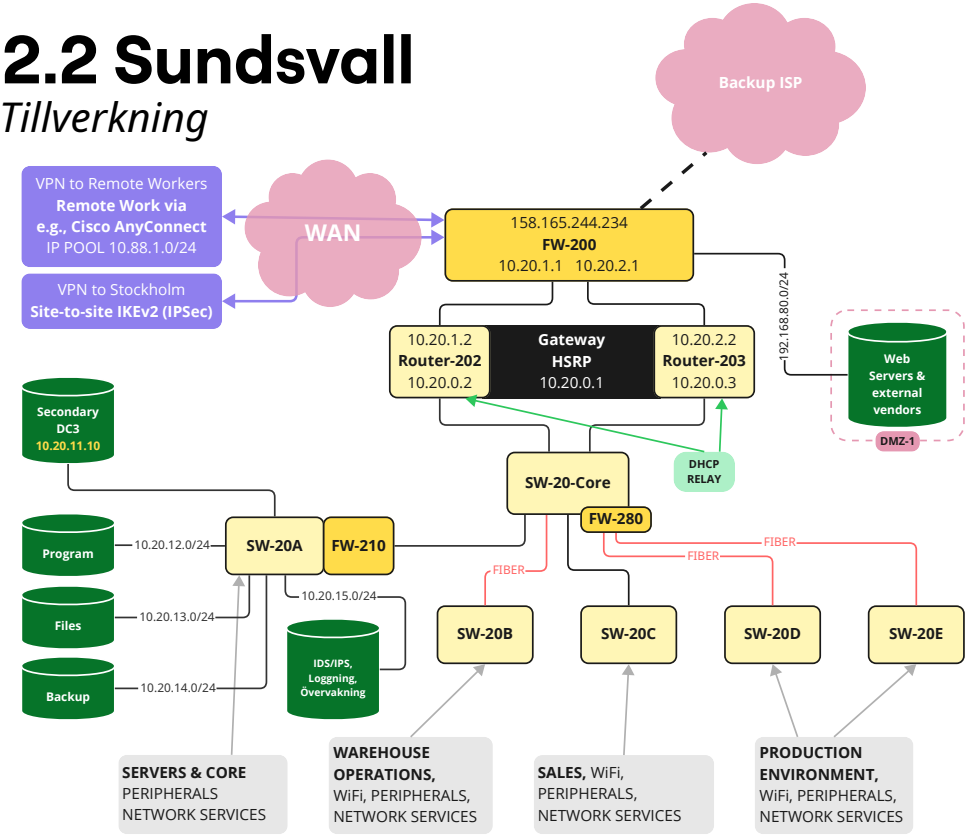
WiFi
- **10.10.71-72.0/24**

PERIPHERALS
- **10.10.90-91.0/24**
- **10.10.96.0/24**

NETWORK SERVICES
- **10.10.97-99.0/24**

2.2 Sundsvall

Tillverkning



SUNDSVALL: VLAN

DMZs
- **80 DMZ-1** Web server / services

SERVERS & CORE
- **211** Domain controllers
- **212** Software / internal services
- **213** Static file storage
- **214** Backup infrastructure
- **215** IDS/IPS, övervakning, logging

WAREHOUSE OPERATIONS
- **221** Workstations/terminals
- **222** Wireless devices/scanners

SALES & MARKETING
- **231** Workstations
- **232** VoIP

WiFi
- **271** Employee-Wireless
- **272** Guest-Wireless

PRODUCTION ENVIRONMENT
- **280** Main prod control systems
- **281** Production quality control
- **282** Production maintenance
- **283** Raw material handling
- **284** Machine controllers
- **285** Packaging

PERIPHERALS
- **290** Printers
- **291** Embedded Devices (IoT)
- **296** Physical Security Systems

NETWORK SERVICES
- **297** Backup/disaster recovery
- **298** Logging and monitoring
- **299** Network-wide management

SUNDSVALL: SUBNETTING

DMZ
- **192.168.25.0/24** DMZ1-Webb

SUNDSVALL LAN
- **10.20.0.0/16**

SERVERS
- **10.20.11-15.0/24**

WAREHOUSE
- **10.20.21-22.0/24**

SALES
- **10.20.31-32.0/24**

WiFi
- **10.20.71-72.0/24**

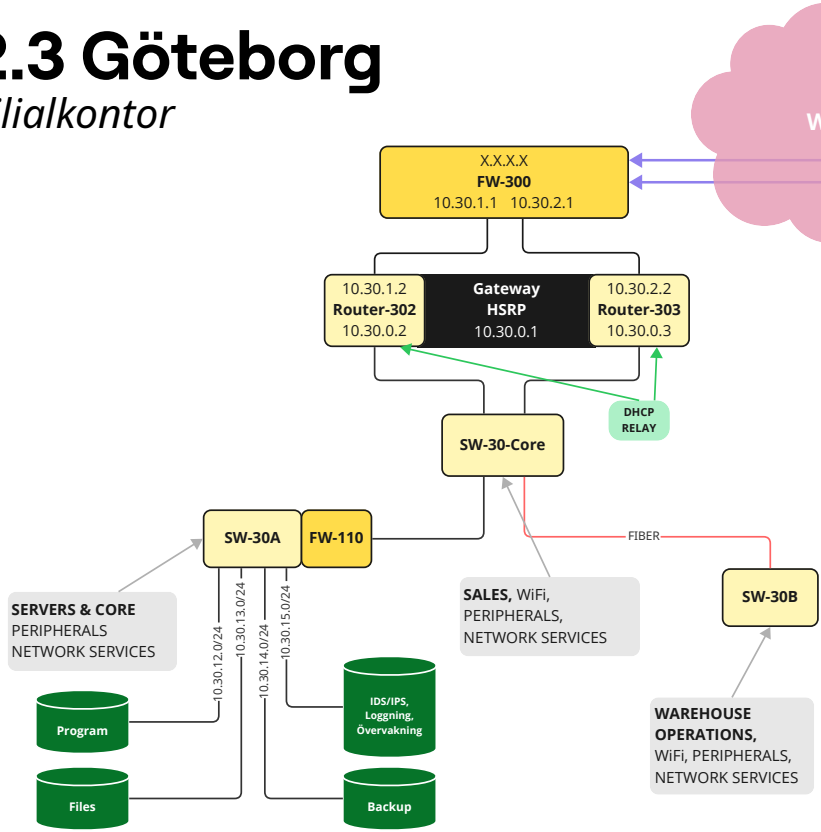
PRODUCTION ENVIRONMENT
- **10.20.80-85.0/24**

PERIPHERALS
- **10.20.90-91.0/24**
- **10.20.96.0/24**

NETWORK SERVICES
- **10.20.97-99.0/24**

2.3 Göteborg

Filialkontor



GÖTEBORG: VLAN

SERVERS & CORE
- **312** Software / internal services
- **313** Static file storage
- **314** Backup infrastructure
- **315** IDS/IPS, övervakning, logging

WAREHOUSE OPERATIONS
- **321** Workstations/terminals
- **322** Wireless devices/scanners

SALES & MARKETING
- **331** Workstations
- **332** VoIP

WiFi
- **371** Employee-Wireless
- **372** Guest-Wireless

PERIPHERALS
- **390** Printers
- **391** Embedded Devices (IoT)
- **396** Physical Security Systems

NETWORK SERVICES
- **397** Backup/disaster recovery
- **398** Logging and monitoring
- **399** Network-wide management

GÖTEBORG: SUBNETTING

GÖTEBORG LAN
- **10.30.0.0/16**

SERVERS
- **10.30.12-15.0/24**

WAREHOUSE
- **10.30.21-22.0/24**

SALES
- **10.30.31-32.0/24**

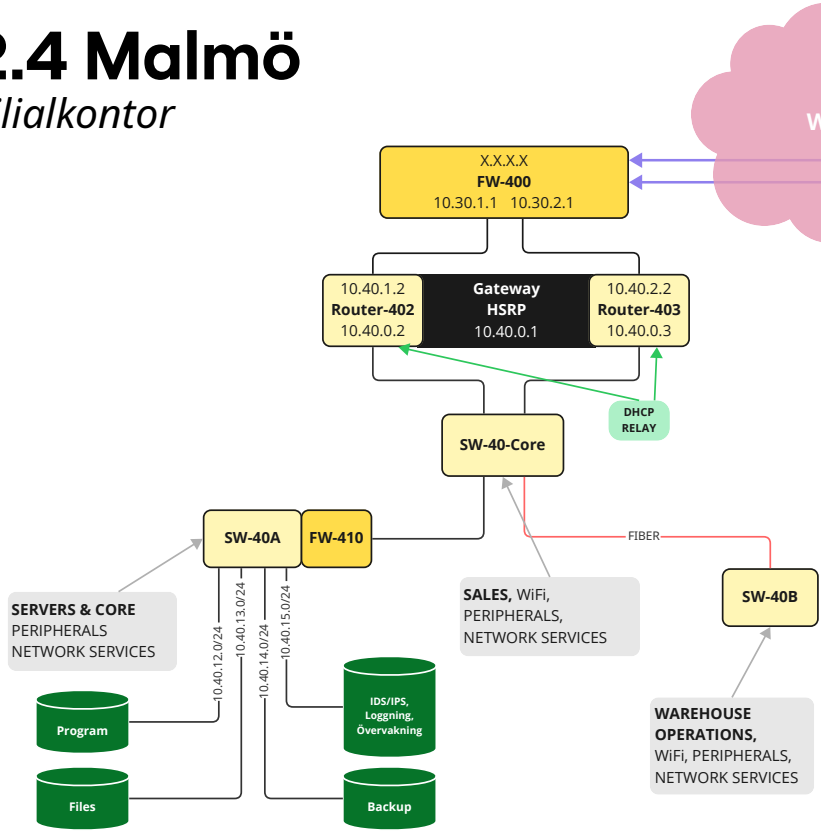
WiFi
- **10.30.71-72.0/24**

PERIPHERALS
- **10.30.90-91.0/24**
- **10.30.96.0/24**

NETWORK SERVICES
- **10.30.97-99.0/24**

2.4 Malmö

Filialkontor



MALMÖ: VLAN

SERVERS & CORE
- **412** Software / internal services
- **413** Static file storage
- **414** Backup infrastructure
- **415** IDS/IPS, övervakning, logging

WAREHOUSE OPERATIONS
- **421** Workstations/terminals
- **422** Wireless devices/scanners

SALES & MARKETING
- **431** Workstations
- **432** VoIP

WiFi
- **471** Employee-Wireless
- **472** Guest-Wireless

PERIPHERALS
- **490** Printers
- **491** Embedded Devices (IoT)
- **496** Physical Security Systems

NETWORK SERVICES
- **497** Backup/disaster recovery
- **498** Logging and monitoring
- **499** Network-wide management

MALMÖ: SUBNETTING

MALMÖ LAN
- **10.40.0.0/16**

SERVERS
- **10.40.12-15.0/24**

WAREHOUSE
- **10.40.21-22.0/24**

SALES
- **10.40.31-32.0/24**

WiFi
- **10.40.71-72.0/24**

PERIPHERALS
- **10.40.90-91.0/24**
- **10.40.96.0/24**

NETWORK SERVICES
- **10.40.97-99.0/24**

3.1.1. Nätverkssegmentering, ACL & VPN

VLAN och segmentering

→ Begränsa åtkomst genom att segmentera nätverket i flera logiska VLAN.

→ **Förenklar** både routing, ACL-konfiguration och felsökning.

→ Varje VLAN kopplas till en motsvarande **/24-subnet**.

→ Dedikerade VLAN för backup, loggning och nätverksadministration, vilket ytterligare stärker säkerheten och driftsäkerheten.

Brandväggar och accesslistor

→ Segmeteringen gör det möjligt att skapa brandväggsregler och accesslistor mellan olika segment.

→ Skydda både utifrån och internt.

→ Externt filtrerar brandväggen all trafik från internet och tillåter bara det som är nödvändigt.

→ Internt **accesslistor (ACLs)** kontrollerar trafiken mellan VLAN.

→ Minimerar lateral rörelse vid ett intrång och följer principen om **minsta möjliga åtkomst**.

VPN-konfiguration

→ Använder **site-to-site VPN** med IKEv1/IPSec.

→ Konfigurerar **transform-set** vilket specificerar krypterings- och integritetsalgoritmer.

→ Varje tunnel är konfigurerad med **AES-256-kryptering**, **MD5-hashning**, och **pre-shared keys** för autentisering.

→ Trafiken som tillåts genom tunneln är strikt reglerad via **access-lists**.

3.1.2. Wi-Fi-konfigurationer, HSRP & övrigt

Wi-Fi-säkerhet

→ Tre nät: ett säkert för anställda, ett isolerat gästnät, samt ett nät för trådlösa enheter i lagret.

→ Vi använder **dynamisk VLAN-tilldelning** via vår Wi-Fi-controller.

→ När användaren loggar in via **802.1X och RADIUS** placeras de automatiskt i rätt VLAN beroende på **behörigheter i AD**.

→ Det här skapar både **bättre säkerhet** och **enklare hantering**, eftersom vi inte behöver ha separata SSID:n för varje grupp.

NAC-principer. Identitet avgör åtkomst istället för enhetens plats i nätet. Det gör Wi-Fi lika säkert som ett segmenterat nät.

Hot-Standby Routing och DHCP-relay

→ **HSRP** för redundant gateway: 10.10.0.1 mellan två routrar.
→ Säkerställer **hög tillgänglighet**.

→ Vår **DHCP-server är centraliserad**, men används av flera VLAN.

→ Konfigurerat **DHCP Relay** på routrarna så att klienter i andra VLAN får IP-adresser korrekt, även om de inte är direkt kopplade till servern.

Övriga konfigurationer

→ ?????

3.2.1. Certifikathantering (PKI)

Intern + Extern CA: En realistisk strategi för Charta

Intern CA används för interna behov:

→ Wi-Fi (802.1X), VPN (EAP-TLS), interna servrar.

→ Integrerat med Active Directory för smidig hantering.

Publik CA för externa tjänster:

→ Webbapplikationer, e-postreläer, fjärråtkomst.

→ Certifikat från t.ex. Let's **Encrypt** eller **Digicert.**

Livscykelhantering av certifikat

Om verksamheten växer behövs bättre översikt och automation:

Microsoft AD CS med autoenrollment för intern miljö.

Let's Encrypt med automatiserad förnyelse (ACME).

HashiCorp Vault för avancerad hantering.

3.2.2. Loggning, övervakning & autentisering

Logging & Övervakning med Syslog

Syslog centraliserar loggning från routrar, switchar och brandväggar.

Skapade en **dedikerad VLAN/subnet** för loggning och övervakning.

Servern samlar in **systemloggar**, **VPN-status**, **åtkomstförsök** och **brandväggshändelser**.

Centralt övervakningsnav.

Content Filtering

Blockerar skadliga domäner och IP-adresser via brandväggsregler.

Skyddar mot phishing och minskar risken för malware-attacker.

MFA

Använder **Microsoft Authenticator** för att säkerställa inloggning till företagskonton och VPN.

802.1X-autentisering plus RADIUS via AD

802.1X-autentisering används för Wi-Fi.

Användarens behörighet kontrolleras via **RADIUS**, som i sin tur kopplas till **Active Directory** (AD).

Det är så ni möjliggör **dynamisk VLAN-tilldelning** – genom att RADIUS returnerar rätt VLAN-ID beroende på grupp i AD.

3.2.3. SIEM: Insamlar, identifierar & larmar

SIEM-system

Samlar och analyserar säkerhetsloggar från brandväggar, routrar, switchar och servrar.

→ Hjälper oss att upptäcka avvikelser, hot och intrång i realtid.

→ Loggar skickas till ett centralt övervakningssystem (Syslog + SIEM).

→ Ger bättre insyn och snabbare incidentrespons.

Snort IDS/IPS

Snort används som vårt Intrusion Detection and Prevention System.

→ Övervakar nätverkstrafik och identifierar misstänkt aktivitet.

→ Blockerar eller loggar trafik baserat på regler.

→ Installeras i ett separat VLAN tillsammans med SIEM-loggning.

Sårbarhetsskanning

Skannar nätverket efter kända sårbarheter i system och enheter.

→ Identifierar felkonfigurationer och bristande patchning.

→ Hjälper till att förebygga attacker innan de sker.

→ Regelbundna skanningar planeras, särskilt på huvud-kontoret i Stockholm.

SIEM --> Splunk, Microsoft Sentinel, Elastic Security (ELK Stack)

3.2.4. Återställning & backup

Disaster Recovery Plan (DRP)

Plan för återställning vid allvarliga incidenter.
→ RTO* och RPO* anpassade efter varje kontors behov.
→ **Hur lång tid** verksamheten **kan vara nere** utan att det orsakar oacceptabel skada.).
→ **Hur gammal den senaste backupen får vara** när vi återställer systemet.

*Recovery Time Objective, *Recovery Point Objective

Backupstrategi

Daglig säkerhetskopiering av kritiska system.

→ Servrar i Stockholm backas upp med t.ex. **Veeam/Acronis**.

→ Krypterad offsite-backup till molntjänst.

→ Versionhantering aktiverad för skydd mot ransomware.

Skydd per plats

Stockholm
Full serverbackup och fjärråterställning.

Sundsvall
Lokala säkerhetskopior med veckosynk till Stockholm.

Göteborg & Malmö
Klientbackup lagras lokalt och synkas regelbundet till Stockholm.

4. Utrustnings- och programvarulista

Hårdvara

Routrar
Med stöd för HSRP (redundant gateway) DHCP Relay för centraliserad adresshantering.

Switchar
Core- och access-switchar med VLAN-stöd, fiberuplinks. Redundans-rekommendation via Spanning Tree.

Brandväggar
Cisco ASA (med stöd för ACL, VPN)

Accesspunkter
WPA3 och 802.1X (stöd för RADIUS-autentisering)
Stöd för dynamisk VLAN-tilldelning

UPS (avbrottsfri kraftförsörjning)
För servrar och kärnnätverk

Mjukvara

Cisco IOS: För switchar och routrar.

Cisco ASA OS:
För brandväggar.

Cisco Packet Tracer: För design, konfiguration och testning.

AnyConnect:
VPN-klient för fjärranvändare.

Windows Server:
AD, DNS, DHCP, filserver, CA.

RADIUS/NPS: För 802.1X och dynamisk VLAN-tilldelning.

Syslog + SIEM:
Logghantering och hotidentifiering.

Snort eller Suricata:
IDS/IPS-tjänster.

Veeam / Acronis:
Backup och återställning.

Let's Encrypt:
Publika certifikat för externa tjänster.

Microsoft AD CS:
Intern certifikat-hantering (PKI).

DNS-filter / Content Filtering: Skydd mot phishing och olämplig trafik.

Servrar

Domain Controllers (Active Directory)
Autentisering och auktorisering. Intern CA (ex. Microsoft AD CS). Möjlighet till integration med publika CA (Let's Encrypt).

Filserver
Central lagring och versionshantering.

Backupserver
Kör t.ex. Veeam eller Acronis
Krypterad offsite-backup (moln).

IDS/IPS-server
Snort eller Suricata.

E-postgateway
I DMZ (filtrerar utgående/intern e-post).

Affärssystem
T.ex. lönesystem eller ERP-tjänst.

Syslog/SIEM-server
Central logg-insamling från brandväggar, routrar, switchar.

5.1.1. Riskbedömning och åtgärder

Risknivå: Hög

A. Single Point of Failure i Core-switchen

Risk: Om **SW-10-Core** går ner eller får ett fel (t.ex. strömavbrott, hårdvarufel), så förlorar hela nätverket sin interna routing och VLAN-kommunikation.

Konsekvens:
→ Kommunikation mellan VLAN upphör.
→ Ingen åtkomst till servrar, internet, backup eller andra segment.
→ Kan orsaka totalt avbrott för hela kontoret.

Åtgärder i vår design (eller rekommendation):
→ Just nu finns **ingen redundans** för core-switchen – vilket är en tydlig sårbarhet.

Nästa steg:
(1) Införa redundant core (t.ex. SW-10-CoreA + SW-10-CoreB) med spanning-tree failover.
(2) Införa LACP i första hand i switcharna till productions-miljö och servrarna för lastbalansering, öka bandbred och skapa redundans.

Risknivå: Medelhög

B. Överbelastning av centrala brandväggarna

Risk: All trafik till/från internet passerar genom en enda brandvägg. Om den överbelastas kan det orsaka flaskhalsar eller säkerhetshål.

Konsekvens: Begränsad tillgänglighet, risk för intrång, eller att kritiska tjänster blockeras felaktigt.

Åtgärder i vår design:
→ **Brandväggsregler (ACLs)** begränsar åtkomst strikt mellan segment och från internet.
→ **Segmentering** gör att endast nödvändig trafik behöver gå genom brandväggen.
→ Vi har en **backup ISP** som redundans för tillgänglighet.

Nästa steg: Lägg till en sekundär brandvägg i en Active/Standby-par (t.ex. **FW-101** med FHRP)

5.1.2. Riskbedömning och åtgärder

Risknivå: Medelhög

C. För stort beroende av dynamisk VLAN-tilldelning via RADIUS

Risk: Om AD eller RADIUS-servern är otillgänglig, får inte användare rätt VLAN vid Wi-Fi-inloggning.

Konsekvens: Användare kopplas inte upp eller får fel nätverksåtkomst (t.ex. gäst i internnät).

Åtgärder i vår design:
→ Dynamisk VLAN-tilldelning via **802.1X + RADIUS + AD**.
→ Styr åtkomst med **NAC-principer** (Network Access Control).
→ Genom att ha fallback-SSID eller lokal fallback-VLAN på Wi-Fi-controller, minskas effekten vid RADIUS-fel (kan förtydligas i presentationen).

Nästa steg: Fixa fallback-SSID eller lokal fallback-VLAN på Wi-Fi-controller

Risknivå: Låg

D. Centraliserad DHCP och en enda gateway (HSRP)

Risk: Om båda routrarna går ner eller DHCP-relay-konfigurationen misslyckas, kan flera VLAN inte få IP-adresser.

Konsekvens: Klienter i flera VLAN tappar nätverksåtkomst helt, vilket påverkar drift och tillgänglighet.

Åtgärder i vår design:
→ **HSRP används för redundans**, där två routrar delar på rollen som gateway (10.10.0.1).
→ **DHCP-relay är konfigurerat** så att alla VLAN ändå kan få IP-adress från en central DHCP-server.
→ Vi minskar risken för singelpunktsfel i routing och adresstilldelning.

Frågor och synpunkter