TEKNISK BESKRIVELSE

IT-infrastruktur og netværkssikkerhed med Fortinet

Introduktion

DTU Science Parks netværksløsning giver hver lejer et dedikeret netværk, adskilt fra andre lejeres netværk. Som en del af grundydelsen er lejerne beskyttet af en fælles firewall med opsatte regler og policies baseret på best practice.

Brugere af løsningen kan frit benytte det trådløse netværk i alle DTU Science Parks bygninger, uanset hvilken virksomhed de er tilknyttet. For eksempel kan en bruger fra Virksomhed A, der har kontor i Bygning A, også tilgå det trådløse netværk i Bygning B eller andre bygninger, hvor løsningen er implementeret.

Derudover kan fysiske netværksstik tilkøbes til udstyr, der ikke understøtter trådløs forbindelse.

Fysisk design

For at sikre høj netværkstilgængelighed er infrastrukturen opbygget med fuld redundans på både Gateway/Firewall-laget og Core-laget i et High Availability-setup på firewalls og core-switche. Internetforbindelsen leveres via to uafhængige fiberforbindelser til ISP-edge.

Access-laget er ligeledes opbygget med redundans, hvor de to Access-switche i hvert krydsfelt er forbundet både indbyrdes og til Core-switche i en ring-topologi. Derudover er WiFi Access Points (AP) tilsluttet, så hvert andet AP er koblet til henholdsvis Access Switch 1 og Access Switch 2 i krydsfeltet. Dette sikrer, at hvis én Access-switch bliver utilgængelig, vil de to nærmeste AP'er fortsat fungere. I en sådan situation kan netværket være degraderet, men forbindelsen opretholdes.

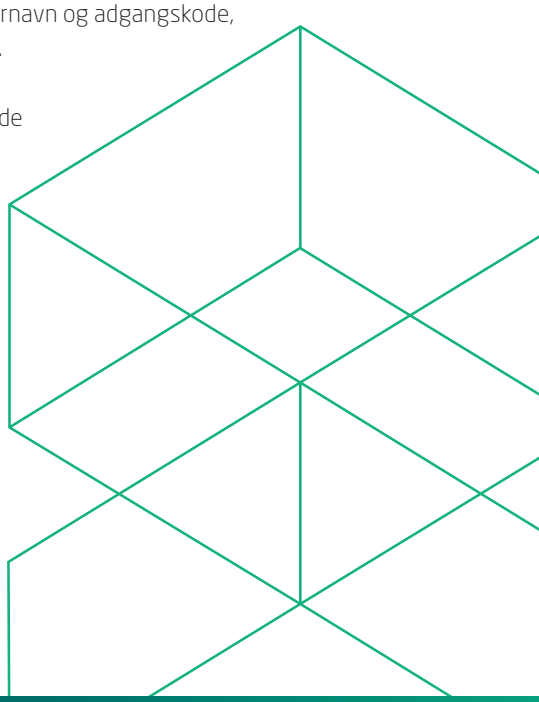
Logisk design

Netværket er segmenteret logisk, så hver lejer tildeles et separat VLAN. Dette sikrer, at lejernes netværk er adskilt, og at det ikke er muligt at tilgå eller se andre lejeres netværk.

For at administrere netværksadgang er der implementeret Network Access Control (NAC), som sikrer, at kun autentificerede enheder får adgang til netværket. Autentificerede enheder tildeles kun adgang til de netværkssegmenter, de er godkendt til.

Desuden er der implementeret en Authentication Service, som knytter enheder til brugere. I praksis betyder det, at brugere skal være oprettet i en bruger-database. Ved tilslutning til netværket vil de blive bedt om brugernavn og adgangskode, hvorefter de – ved godkendelse – tildeles adgang til deres respektive netværkssegment(er).

Dette design gør det muligt for brugerne at få adgang til deres eget netværk, uanset hvor de befinder sig inden for de dækkede områder.



Tekniske specifikationer

Internetadgang

Internetforbindelsen leveres via fiber fra to geografisk adskilte ISP-edge, ført ind i to forskellige bygninger og hovedkrydsfelter. Systemet er designet med automatisk failover ved hjælp af BGP og HSRP, hvilket sikrer, at trafikken automatisk skifter til den sekundære forbindelse i tilfælde af nedbrud.

Firewalls

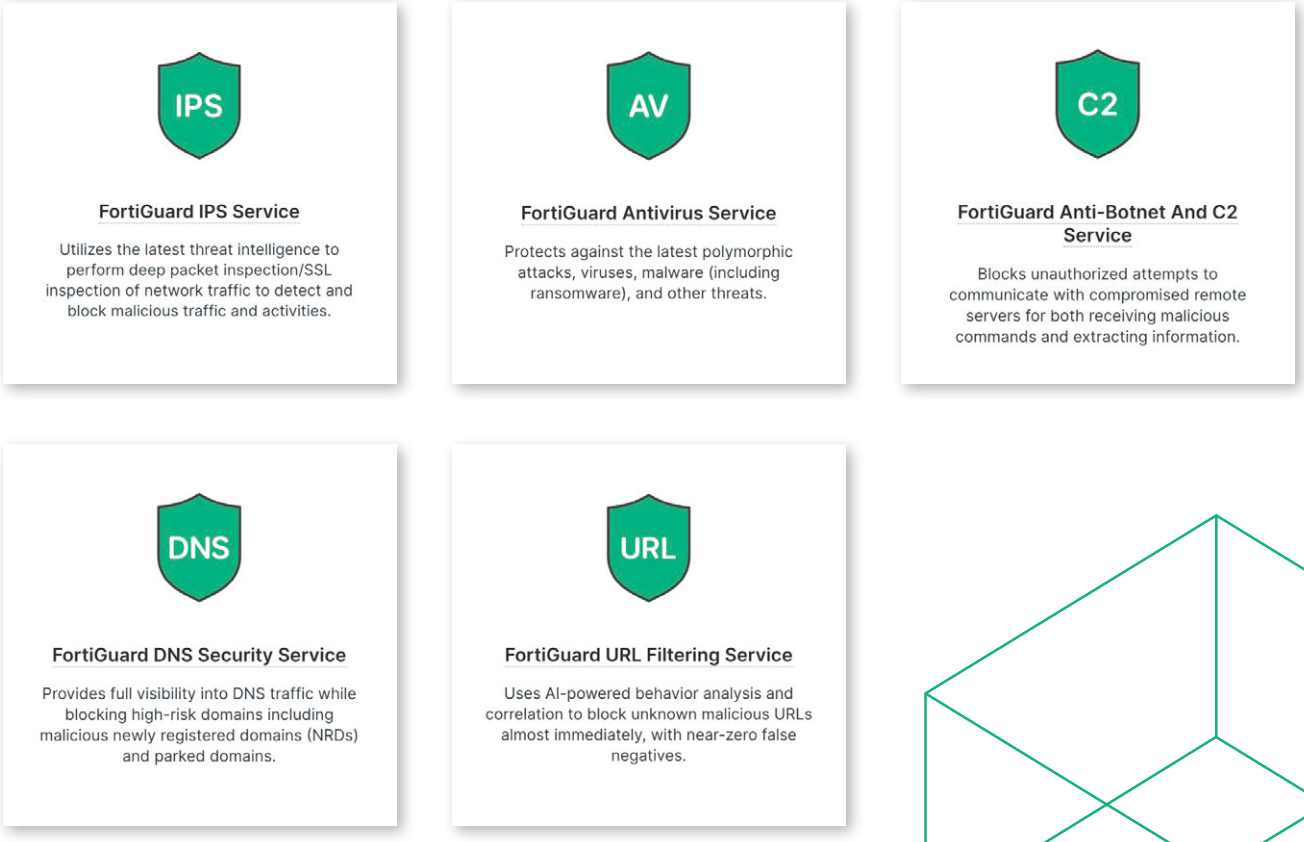
Netværket er sikret med Fortinet FortiGate NGFW, der inkluderer Unified Threat Protection. FortiGate er kendt for sin høje sikkerhed og ydeevne og beskytter effektivt mod netværkstrusler og angreb.

De primære firewalls er udstyret med 100G WAN-interfaces, hvor internetforbindelserne termineres. De er konfigureret i et High Availability-setup, så den sekundære firewall automatisk overtager ved fejl eller nedbrud.

FortiGate er integreret med FortiGuard AI-powered Security Services, som leverer følgende beskyttelsesfunktioner:

- Intrusion Prevention System (IPS)
- Advanced Malware Protection (AMP), inklusive:
  - Antivirus
  - Botnet-detektion
  - Mobile malware-beskyttelse
  - Outbreak Prevention
- Web Security, inkl.:
  - Web- og indholdsfiltrering
  - Secure DNS-filtrering
  - Video-filtrering

Klik på ikonerne nedenfor for at læse mere om de enkelte FortiGuard-services.



Core-lag

Core-lagets switche er, ligesom firewalls, konfigureret i et High Availability-setup og er redundant forbundet til begge firewalls. Core-switche har flere SFP+-interfaces, der anvendes til cross-connects og tilslutning af Access-switche.

Access-lag

Access-laget består af Access-switche og WiFi Access Points (AP'er).

Access-switche installeres parvis og er direkte forbundet. Alle switch-par er koblet sammen i en ring-topologi, hvor hver enhed har forbindelse til både Core-switche og andre Access-switche. Dette sikrer, at et eventuelt nedbrud af en switch ikke påvirker resten af netværket.

WiFi Access Points (AP'er) tilsluttes skiftevis til hver af de to Access-switche i et par. Hvis en af switchene bliver utilgængelig, vil kun hvert andet AP være påvirket. Brugerne vil stadig have adgang til WiFi, dog muligvis med reduceret hastighed og kvalitet.