Hedmark IKT
Et interkommunalt IKT-samarbeid

Anskaffelse av brannmurløsning for Hedmark IKT

Innhold

1. Innledning

1.1 Dagens løsning

Dagens brannmurløsning består av en ytre og indre brannmur (et ytre og indre cluster). Linknett mellom ytre og indre brannmur består av et vlan på en L2-link via kjerneswitcher.

Administrasjon gjøres primært via Web-GUI men også med CLI.

Dagens løsning er basert på L3-linker mot utelokasjoner med egen vpn-konsentrator med linknett mot både ytre og indre brannmur. Sentralt på serverrom brukes L2 og vlan via Dell-switcher. All trafikk rutes i sentral brannmurløsning. IPv4 er fortsatt primært brukt men IPv6 er tilgjengeliggjort fra ISP og på vei inn for test. Ruting er primært statisk med noe bgp for redundans mot for eksempel ISP.

Det er ca. 290 utelokasjoner som benytter Fortigate. VPN-cluster og ytre brannmur-cluster er Fortigate. Indre brannmur-cluster er av typen Sonicwall.

I dagens brannmurløsning benytter vi blant annet sikkerhetsmekanismer som IPS, IDS, antivirus, ssl offloading, ssl-vpn, lastbalansering/virtual server.

Serverparken består av et blandet miljø med virtuelle og fysiske Linux- og MS Windows-servere. De virtuelle serverne kjører på VMWare ESXi og XEN med delt lagring (iSCSI).

1.2 Mål for løsning

Hedmark IKT ønsker å ha en fremtidsrettet og enhetlig brannmurløsning med kapasitet til å vokse i. Vi har pr. i dag en god internkompetanse på Fortigate.

I tillegg til å beskytte en rekke servernett og flere ulike DMZ for trafikk fra internett vil løsningen benyttes til å regulere trafikk mellom de ulike sikkerhetssonene, inkludert å beskytte resten av nettverket mot uønsket trafikk fra brukernettene.

Tilbudt løsning skal være 2 stk separate fysiske hardwarechassis/appliance i cluster for redundans.

Tilbudt løsning skal erstatte de deler av dagens brannmurløsning som ikke er Fortigate. Hedmark IKT ønsker å etablere en mest mulig enhetlig og brannmur- og VPN løsning.

Vi anser det som en viktig del av leveransen å inkludere en god, sikker, stabil og forutsigbar brannmurløsning som tar høyde for et voksende trafikkbehov og 24-timers drift.

Ved SW-oppgraderinger skal det heller ikke være nødvendig med opplevd nedetid.

I en serviceavtale ønsker Hedmark IKT godt dokumenterte supportrutiner og en eskaleringsstige, slik at det før kontraktsinngåelse er klarlagt hvilke offisielle veier man skal bruke for feilmelding og eventuell eskalering av problemer.

2. Hedmark IKTs tekniske arkitektur og løsninger

2.1. Teknisk Plattform

Hedmark IKT har en serverpark som består av et blandet miljø med virtuelle og fysiske Linux- og MS Windows-servere. De virtuelle serverne kjører på VMWare ESXi eller XEN med delt lagring (iSCSI).

Noen grunntall for miljøet pr. oktober 2018:

Virtuelt miljø basert på VMware og XEN:

- Ca. 500 stk. Virtuelle servere

Fysiske servere:

- Ca. 60 stk.

Nettverk:

- Sentralt serverrom:
  - Dell Force10 kjerneswitcher
  - Dell N3000&4000 serie kantswitcher
  - 2stk. Fortigate 1200D cluster (ytre brannmur), 2stk. Sonicwall NSA6600 cluster (indre brannmur), 2stk. Fortigate 1200D cluster (vpn-konsentrator)
- Lokasjoner:
  - Ca. 290 lokasjoner
  - Ca. 800 switcher av ulike Dell og Cisco-modeller.
  - Ca. 250 Fortigate 60D/80E (L3 ipsec vpn)
  - Ca. 1700 WiFi aksesspunkter

Sluttbrukerinformasjon:

- Ca. 20000 brukere
- Ca. 8000 nettbrett
- Ca. 4500 pc'er
- Ca. 3000 gjesteenheter i døgnet

Hedmark IKT har en sonemodell som baseres på en indre og en ytre sone.
Lokal infrastruktur på datasenter er blandet 1GBit over RJ45, og 10Gbit over SFP+.
Traversering av brannmurer med backuptrafikk må begrenses i den grad det er mulig.

3. Krav til avtalepartner

Våre krav til avtalepartner for anskaffelsen:

3.1. Kompetanse.

- Kompetanse på tilbudt løsning skal dokumenteres i form av leverandørens generelle kompetanse innen brannmur i form av prosjekter, kundeportefølje, leveranser til de ulike kunder. Kompetansen på de ressurser som tilbys Hedmark IKT som del av tilbudet, skal også beskrives i form av CV eller tilsvarende.
- Referanse fra minimum tre tilsvarende inngåtte avtaler de siste tre år skal oppgis.

3.2. Support og service.

- Standard responstider ved feilsituasjoner skal oppgis
- Supportapparat, inklusive eventuelle underleverandør skal beskrives
- 24/7-365 support
- Oppdragsgiver skal kunne forholde seg til en leverandør ved support henvendelser (SPOC)

Leverandør skal beskrive og dokumentere sin løsning for dette.

3.3. Leveranseapparat.

- Godt leveranseapparat
- Standard leveringstider fra bestilling er sendt fra oppdragsgiver skal oppgis
- Regime for sanksjoner ved forsinkelser, eller manglende leveranser skal oppgis
- Beskrivelse av kompetanse hos konsulenter.

Leverandør skal beskrive og dokumentere sin løsning for dette.

3.4. Opplæring og rådgivning.

- Opplæring av oppdragsgivers ansatte, både for innføring av nye rutiner og tekniske løsninger, skal beskrives. Forslag til gjennomføring av denne opplæringen med forpliktende priser, skal oppgis i vedlegg «Prisskjema».
- Opplæring internt eller eksternt av minimum 8 deltakere
- Opplæringen på feilsøking av løsningens komponenter. Minimum 6 deltakere.

Leverandør skal beskrive og dokumentere sin løsning for dette.

3.5. Konsulenttjenester

- Oppdragsgiver ønsker pris på konsulenttjenester.
    - Forpliktende timepris for uttak av konsulentbistand i kontraktsperioden

Leverandør skal opplyse om timepris i vedlegg «Prisskjema».

4. Tekniske krav

4.1. Funksjonalitet påkrevd i løsningen

- Tilbudt løsning skal enten være av type Fortigate eller tilsvarende som fungerer godt sammen med Fortigate
- Tilbudt løsning må ha minimum 80 Gbps brannmur throughput per hardwareenhet
- Hver hardwareenhet i tilbudt løsning må ha minimum 8 stk 10 Gbps Sfp+ interfaces og minimum 10 stk 1Gbps RJ45
- Tilbudt løsning må støtte minimum 12.000.000 samtidige sesjoner/connections per hardwareenhet
- Tilbudt løsning må være i stand til å håndtere minimum 300 000 nye sesjoner/connections per sekund
- Tilbudt løsning skal støtte VIP/MIP, NAT, IPv4, IPv6, snmp, syslog til dedigert loggserver
- Tilbudt løsning må være redundant med 2 stk fysiske «next generation» brannmurer i active/standby eller active/active-oppsett med støtte for
    - Malware protection
    - IPS/IDS
    - Ddos protection
    - Applikasjonsscanning
    - Antivirus
    - SSL-offload
    - Lastbalansering/virtual server
- Tilbudt løsning må ha både Web-GUI og CLI grensesnitt
- Tilbudt løsning må ha mulighet for ldap e.l. for tilkobling mot AD og styring av brukertilganger
- Tilbudt løsning må støtte statisk ruting og dynamisk ruting som bgp, ospf osv
- Tilbudt løsning må kunne eksportere/importere konfigurasjon via kryptert tilgang (ssh,sftp ol)
- Tilbudt løsning må kunne deles inn i flere virtuelle brannmurer

Leverandør skal beskrive sin løsning for disse kravene over.

4.2. Funksjonalitet ønsket i løsningen

- Gode muligheter for å hente ut rapporter
    - Ytelse og kapasitets monitorering
    - Ekstra logging og rapporteringsmuligheter
- Web-filtrering
- Gode varslingsmuligheter ved hendelser i løsningen utover snmp og syslog
- Tilbudt løsning bør ha mulighet for å benytte clustering e.l. for å øke løsningens totale ytelse, ved å utvide antall hardwareenheter ut over 2 enheter
- Hver hardwareenhet i tilbudt løsning bør støtte redundante PSUer og leveres med minimum to PSUer

Leverandør skal beskrive sin løsning for ønskede funksjoner.

5. Implementering

5.1. Installasjon

- Installasjon av valgt løsning foretas av oppdragsgiver med bistand fra leverandør. Omfanget av bistand fra leverandør vil avhenge av tilbudt løsning sett opp mot Hedmark IKT sin etablerte internkompetanse.
- Leverandør skal beskrive sin plan og estimert omfang for installasjon av tilbudt løsning.