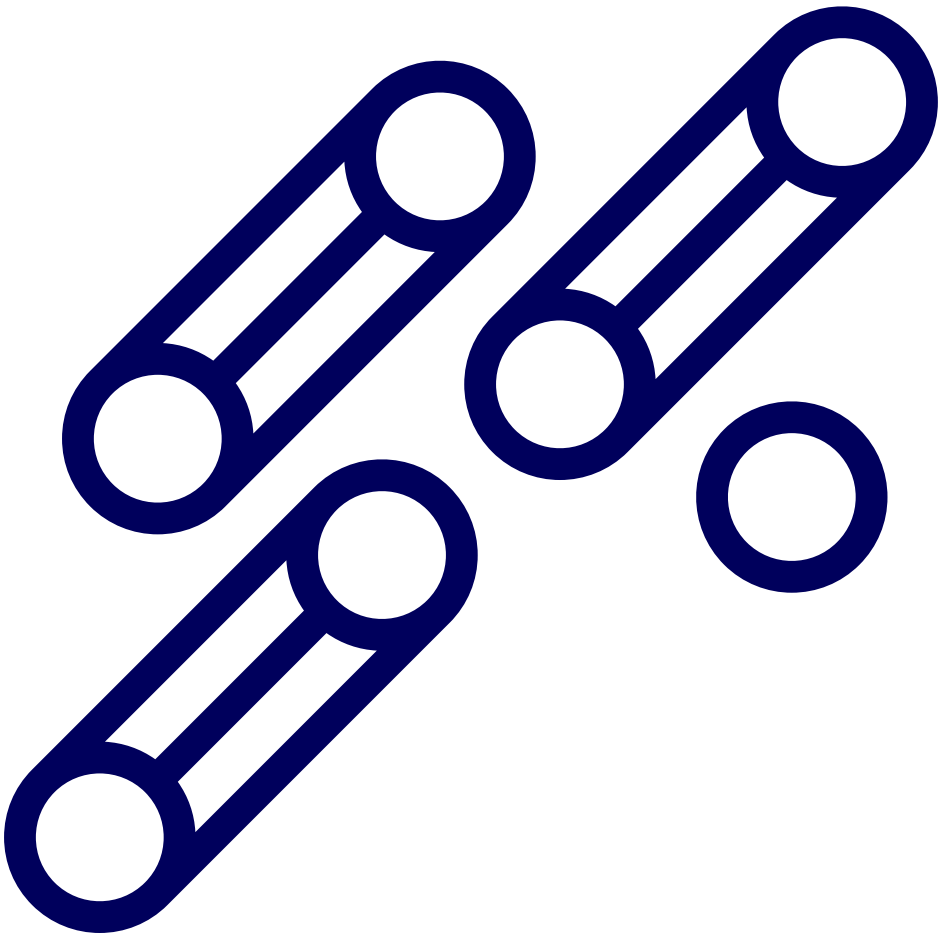


Tjenestebeskrivelse

Nettsentrisk brannmur

4.7.2019

GlobalConnect

Table of contents

1 Innledning

Denne tjenestebeskrivelsen beskriver en Nettsentrisk brannmurstjeneste fra GlobalConnect.

For mange er IT-sikkerhet komplisert og distraherer virksomheten i den daglige driften. Med Nettsentrisk sikkerhet tilbyr GlobalConnect ***sikkerhet levert som en tjeneste*** til virksomheter.

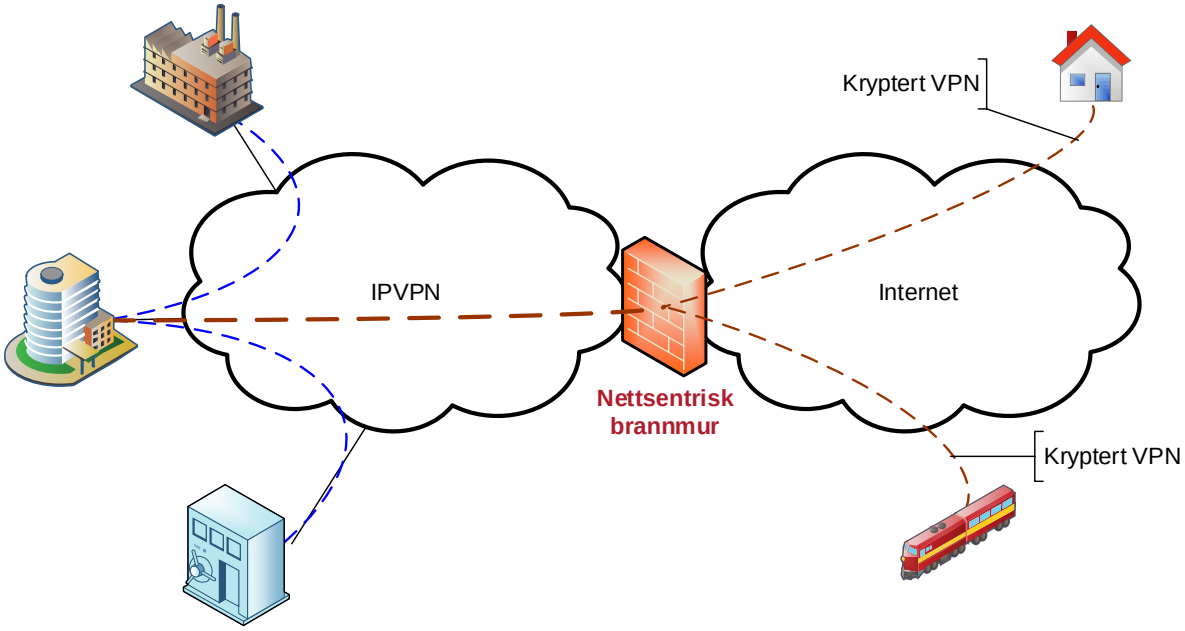
Med markedsledende teknologier og solid kompetanse tilbyr vi kosteffektive løsninger som sparer kunden for investeringer i hardware, software og egne driftsressurser. Med nettsentriske sikkerhetsløsninger fra GlobalConnect vil uønsket trafikk stoppes før den når kundens aksessforbindelse.

Med et uoversiktlig trusselbilde og en økning av angrep mot kritiske tjenester og infrastruktur, er det ikke nok å stole på teknologier alene. Det er essensielt å ha tilgang til kompetanse for å beskytte seg mot trusler. I GlobalConnect har vi samlet ressurser i et operasjonssenter for Nettverk og Sikkerhet (NOC/SOC) som jobber 100 % med å beskytte kunder og infrastruktur.

Som del av vår sikkerhetsportefølje kan vi levere DDoS-beskyttelse som beskytter virksomheter mot tjenestenektangrep. GlobalConnect DDoS-beskyttelse er beskrevet i eget dokument, ta gjerne kontakt med oss for mer informasjon om tjenesten.

Videre i dokumentet beskrives sikkerhetstjenester for 2 forskjellige IP-nett:

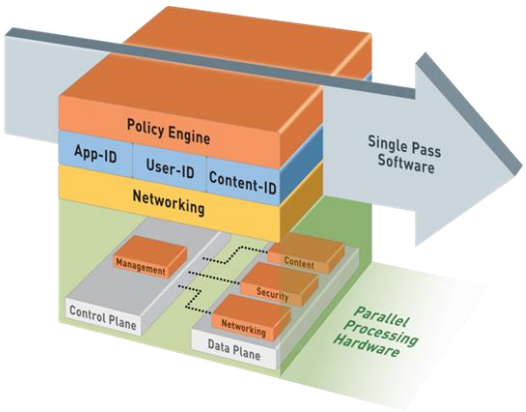
- Nettsentrisk brannmur for IPVPN beskytter det bedriftsinterne nettet mot trusler fra Internett og blokkerer/filtrerer trafikk iht. kundens sikkerhetspolicy. Den nettsentriske brannmuren gir sikker Internettilgang for brukere knyttet til et IPVPN fra GlobalConnect. Funksjonalitet for Nettsentrisk brannmur for IPVPN er beskrevet nærmere i kap. 3.
- Sikker Internett beskytter Internett-aksessen til kunden mot trusler fra Internett og blokkerer uønskede applikasjoner og uønsket innhold. Funksjonalitet for Sikker Internett er beskrevet nærmere i kap. 4.



PRINSIPPSKISSE NETTSENTRISK BRANNMUR FOR IPVPN

2 Om brannmurtjenesten

Brannmurtjenesten identifiserer applikasjoner, innhold og trusler som behandles av et regelsett definert av kunden. Brukere får tilgang til ønsket informasjon og sikres mot trusler fra Internett. Kort oppsummert vil tjenesten:



- Identifisere applikasjoner (App-ID)
- Indentifisere brukere (User-ID)
- Sjekke innholdet (Content-ID)

2.1 Høy tilgjengelighet

Design og løsning er utviklet med tanke på leveranse av tjenester med høy oppetid. Plattformen er geo-redundant med duplisert hardware installert på ulike lokasjoner. Enkelt-feil i arkitektur skal ikke påvirke tilgjengeligheten for kunde.

2.2 Tilpasset regelsett

- Innhold og applikasjoner identifiseres og kan blokkeres basert på type trafikk.
- Sammen med AD[1] kan brukere identifiseres og grupperes for tilgangskontroll
- Innholdet i trafikken skannes for trusler
- For IPVPN-kunder kan konfidensielt innhold ivaretas med kryptering

2.3 Avansert beskyttelse

- Brannmuren sjekker alle applikasjoner for å sikre kommunikasjonen inn og ut av virksomhetens nettverk. Dette reduserer risikoen for angrep
- For IPVPN-kunder kan inspeksjon av SSL-trafikk utføres
- Brannmuren hindrer sofistikerte angrep som benytter flere vektorer (exploit, malware, DNS, command&control, URL m.m.) gjennom kjente innholds-baserte signaturer
- Brannmuren detekterer malware & exploits vha. en signatur-database som oppdateres jevnlig

[1] Active Directory, en katalogtjeneste med brukeridentifikasjon

3 Nettsentrisk brannmur for IPVPN

Tjenesten inkluderer en logisk Internettforbindelse + tjenestefunksjonalitet og består av:

1. Logisk forbindelse til Internett som leveres i hastighets-steg fra 2 Mbps til 1 Gbps
2. For IPVPN finnes 3 definerte funksjonalitetspakker (Standard, Plus og Premium)
3. Enkelte tjenester bestilles som en opsjon og er merket <Opsjon> i tabellen under.

Tjeneste	Standard	Plus	Premium	Beskrivelse
Applikasjonskontroll	√	√	√	Blokkere uautorisert Internettrafikk basert på applikasjonstype.
Applikasjonsbruk	√	√	√	Ser applikasjonsbruken i nettverket. Mulig å sette alarmnivå for brudd på policy.
Standardrapport	√	√	√	Regelmessig rapportering på nettverkstrafikk.
Anti-virus og Anti-Spyware	X	√	√	Beskyttelse mot ondsinnet trussel som kan medføre tap av data og nedetid.
URL-filtrering	X	√	√	Unngå uønsket innhold. Reduserer risiko for brudd på juridiske og regulatoriske forhold. Økt produktivitet.
Tilpasset sikkerhetspolicy	X	√	√	Tilpasser sikkerheten i henhold til bedriftens sikkerhetspolicy. Kan tilpasses individuelle brukere, grupper eller lokasjoner. Krever integrasjon med AD.
Tilpasset rapport	X	√	√	Tilpasset rapport med informasjon til ulike interessenter.
Forebygge inntrenging (IPS)	X	X	√	Beskyttelse mot uautorisert og ondsinnet tilgang som kan resultere i tap av data og nedetid.
Fil-filtrering	X	X	√	Reduserer risikoen for uautorisert filoverføringer inn og ut av bedriftens nettverk.
Sikker fjernaksess	X	Opsjon	Opsjon	Gir brukere utenfor kontoret sikker tilgang til ressurser i bedriftens intern-nett.
Sikker kommunikasjon mellom lokasjoner	X	Opsjon	Opsjon	Sikker kryptert kommunikasjon mellom ekstern lokasjon og bedriftens VPN.
Brukeridentifikasjon	X	Opsjon	Opsjon	Retningslinjer definert i katalogtjeneste (f.eks. Active Directory) kan synkronisere regelsett/policy definert i brannmuren.
Sikkerhetssone	X	Opsjon	Opsjon	Separate soner, f.eks Demilitær sone (DMZ), gjestenett etc.

√ = Inkludert X = Ikke tilgjengelig

4 Sikker Internett

Tjenesten inkluderer sikkerhetsfunksjonalitet for Internettaksesser og består av:

1. Logisk kapasitet gjennom den nettsentriske brannmuren som tilsvarer hastigheten på Internett-aksessen til kunden. Selve internettaksessen bestilles som eget produkt.
2. For Sikker Internett finnes 2 definerte funksjonalitets-pakker:
    a. Internett applikasjonskontroll
    b. Internett beskyttelse

Tjeneste	Internett applikasjonskontroll	Internett beskyttelse	Beskrivelse
Applikasjonskontroll	√	√	Blokkere uautorisert Internettrafikk basert på applikasjons type.
Applikasjonsbruk	X	√	Ser applikasjonsbruken i nettverket. Mulig å sette alarmnivå for brudd på policy
Anti-virus og Anti-Spyware	X	√	Beskyttelse mot ondsinnet trussel som kan medføre tap av data og nedetid.
URL-filtrering	X	√	Unngå uønsket innhold. Reduserer risiko for brudd på juridiske og regulatoriske forhold. Økt produktivitet.
Tilpasset sikkerhetspolicy	X	√	Tilpasser sikkerheten i henhold til bedriftens sikkerhetspolicy. Kan tilpasses individuelle brukere, grupper eller lokasjoner.
Forebygge inntrenging (IPS)	X	√	Beskyttelse mot uautorisert og ondsinnet tilgang som kan resultere i tap av data og nedetid
Fil-filtrering	X	√	Reduserer risikoen for uautorisert filoverføringer inn og ut av bedriftens nettverk.

√ = Inkludert X = Ikke tilgjengelig

Sikker Internett-tjenesten leveres med offisielle IP-adresser tildelt av GlobalConnect. Ønsker kunden å benytte private IP-adresser må NAT[2]-funksjonalitet ivaretas av kundeplassert utstyr.

For dette kan GlobalConnect levere Internett Managed-tjenesten (med kundeplassert ruter) sammen med brannmurtjenesten.

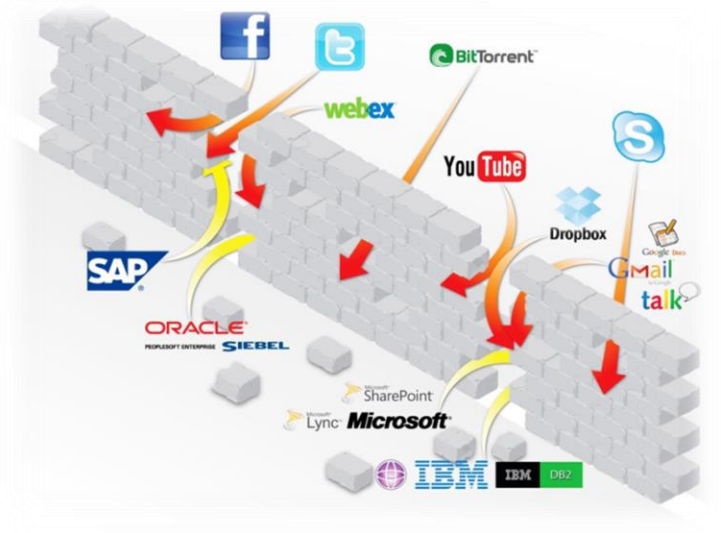
[2] NAT= Network Address Translation

5 Funksjonalitet og opsjoner

Dette kapittelet beskriver og gir eksempler på funksjonaliteten i sikkerhetstjenestene som kan leveres. For spesifikk funksjonalitet som kan bestilles til IPVPN og Internett refereres det til tabellene i kap. 3 og 4.

5.1 Applikasjonsbruk og kontroll

Med App-ID kan du se hvordan programmer i ditt nettverk oppfører seg og relative risiko. Dette gir kontroll over programmer som er skjult som legitim trafikk, bytter porter og/eller er kryptert (SSL og SSH). Slike scenarier er vanskelige å oppdage uten App-ID. App-ID sammen med Content-ID gir ønsket beskyttelsesnivå for forretningskritiske applikasjoner og filer, samtidig som det gir trygghet mot ondsinnede trusler.

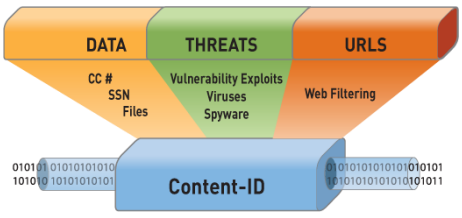


5.2 AntiVirus og Anti Spyware

Utvidet bruk av sosiale medier, meldinger og ikke-arbeidsrelaterte programmer introduserer en trussel og kan brukes til å spre virus og "implementere" programmer som er laget for å infisere eller skade datamaskiner eller nettverk (malware). Den nettsentriske brannmuren tillater kunden å blokkere uønskede programmer med App-ID og deretter skanne de tillatte applikasjoner for malware.

5.3 URL-filtrering

URL-filteret sjekker trafikken mot en lokal database som inneholder mer enn 20 millioner URL-adresser sortert i tilnørmet 60 kategorier (se Appendix 1, URL kategorier). For å sikre maksimal ytelse og minimal ventetid for ofte brukte webadresser gjøres et lokalt oppslag. Finnes ikke adressen gjøres en spørring mot en global database som blir oppdatert med nye nettsteder. Ved å kombinere applikasjonskontroll og URL-filtrering kan fleksible regelsett iverksettes for å kontrollere nettverksaktivitet.



5.4 Fil-filtrering

Fil-filteret kontrollerer strømmen av et bredt spekter med filtyper og ser inn i data-pakkene for å avgjøre om overføring av filen er tillatt iht. kundens sikkerhets-policy. Blokkering av filtype kan

fleksibelt implementeres for enkelt-grupper i en organisasjon. Tatt som et eksempel kan webmail for Gmail tillates brukt for en gruppe, og blokkeres for andre.

5.5 Sikker fjernaksess

Brukere som ikke er direkte tilknyttet VPN-et f.eks. fra hjemmekontor, ansatte på reise og mobile enheter får tilgang til VPN-et med en kryptert forbindelse. IPsec eller SLL benyttes som krypteringsform mellom bruker og kundens VPN.

For sikker kommunikasjon fra lokasjon med flere brukere som ikke er direkte knyttet i VPN-et, benyttes "IPsec Site-to-Site VPN". Dette for å kryptere trafikken som transporteres over Internett før den når kundens VPN.

5.6 SSL de-kryptering

På forespørsel kan trafikk inspiseres ved å de-kryptere ssl sesjoner på brannmuren, innholdet vil med dette kunne sjekkes for Malware. Funksjon krever mer av ytelsen på brannmuren og vil prises på forespørsel.

For å inspisere innkommende trafikk må en kopi av sertifikatet til serveren som skal beskyttes installeres i brannmuren. For å inspisere utgående trafikk må det installeres et sertifikat fra bedriftens "Microsoft Certificate Server". Veiledning for dette vil kommuniseres med teknisk avdeling.

5.7 IPS (Intrusion Prevention Systems)

IPS-funksjonaliteten i brannmuren forebygger inntrenging og blokkerer kjente sårbarheter. Kjernen i systemet er utviklet og vedlikeholdes av erfarne signaturutviklere, som er aktivt med i trussel-beskyttelse av samfunnet. Det utføres pågående forskning og arbeider tett med programvareleverandører, gjennom programmer som f.eks Microsoft Active Protections Program (MAPP).

IPS-funksjonaliteten følger med trafikken på nettverket og stopper unormale hendelser. Et IPS-system gjør det samme som et Intrusion Detection System (IDS). Istedenfor kun å logge hendelser (IDS), vil IPS sette i gang tiltak som respons på hendelsen.

5.8 Rapporter

For IPVPN kunder kan Standard og tilpasset rapport genereres og sendes jevnlig til en avtalt e-postadresse. Rapportene vil gjenspeile informasjon avhengig av funksjoner benyttet i brannmuren (ref. kap.3)

Standard rapporten er en "SaaS application usage report" som oppsummerer applikasjoner på Internett som benyttes av brukere i kundens IPVPN. Fra et sikkerhetsmessig ståsted er applikasjonene vurdert og forbundet med en relativ risiko og rapporten vil vise antall brukere som benytter lav eller høy – risiko applikasjoner.

Tilpasset rapport kan leveres til IPVPN kunder med Nettsentrisk brannmur PLUS eller PREMIUM tjeneste.

Tilgjengelige rapporter for den respektive tjeneste er:

Rapport typer	Standard	Plus	Premium
SaaS application usage report	√	√	√
URL/Web – filter rapport	X	√	√
Threat report	X	√	√

Rapport typer	Standard	Plus	Premium
Data filter report	X	X	√

Ønskes en ytelsesrapport som viser båndbreddeforbruk m.m. vil VPNview være en egnet tjeneste. For mer informasjon, se egen tjenestebeskrivelse for VPNview.

5.9 Brukeridentifikasjon

For identifikasjon av brukere kan brannmurtjenesten integreres med bedriftens katalogtjeneste(AD[3]), som lar deg se brukere av applikasjoner i nettverket. Med dette kan bedriften styre tilganger for grupper og brukere.

5.10 Sikkerhetssone

Bedriftens nettverk kan segmenteres i funksjonelle områder med bruk av sikkerhets-soner. Brannmurens sikkerhetspolicy vil tillate eller blokkere trafikk fra å passere mellom de ulike sonene. En de-militær sone (DMZ) benyttes ofte for tjenester som skal være tilgjengelig fra Internett og bør holdes adskilt fra en sikker internsone. En DMZ benyttes typisk for web-server, email-server og server for fildeling. Trådløse gjestenett er også eksempel på nett som ønskes lagt inn i en egen sone skilt fra det interne nettet.

[3] Active Directory

6 Tjenestekvalitet

Tjenestekvalitet (SLA[4]) er detaljert beskrevet i eget dokument.

Tjenestekvaliteten som tilbys er en kombinasjon av servicetid og Servicegaranti spesifisert for tjenesten. Avtalen spesifisert for Nettsentrisk sikkerhet gjelder for sikkerhetstjenesten og er uavhengig av avtaler inngått for VPN og aksessforbindelser. Under følger en oppsummering av dekningsperiode og Servicegaranti for Nettsentrisk brannmur og Sikker Internett-tjenesten.

6.1 Servicetid

Servicetiden spesifiserer dekningsperioden for feilmelding, feilhåndtering og feilretting. Uten tegning av en spesifikk avtale gjelder servicetid Basis. Ønskes annen servicetid enn Basis bestilles dette som en tilleggstjeneste.

Betegnelse	Type feil som rettes	Servicetid
Basis	Alle	Virkedager kl. 08:00 – 17:00
Utvidet	Alle	Virkedager kl. 07:00-23:00 Lørdager kl. 07:00-23:00
Kontinuerlig	Alle	24/7/365

6.2 Servicegaranti

Servicegaranti spesifiserer responstid for Nettsentrisk sikkerhet. Uten tegning av en spesifikk avtale gjelder Servicegaranti 1 for Nettsentrisk sikkerhet. Ønskes høyere Servicegaranti bestilles dette som en tilleggstjeneste.

Nettsentrisk sikkerhet (brannmur) leveres med følgende Servicegaranti:

Nettsentrisk brannmur	Servicegaranti 1	Servicegaranti 2	Servicegaranti 1
Tjenestetilgjengelighet per kvartal	99,60%	99,75%	99,99%
Responstid	< 2 timer	< 1 time	< 30 minutter
Tilbakemelding	< 2 timer	< 1 time	< 30 minutter
Fysisk feilretting (normal feilrettingstid)	< 8 timer	< 4 timer	< 3 timer
Terminalbasert feilretting (normal feilrettingstid)	< 4 timer	< 3 timer	< 1 time

6.3 Forbehold

Regelsettet implementert for kunden i den Nettsentriske brannmuren er tilpasset kundens sikkerhetspolicy og behov.

Regelsettet implementert er basert på kundens spesifikasjon og kundens eget ansvar.

Opplever kunden feil i regelsett spesifisert av oppdragsgiver, fraskriver GlobalConnect seg ansvaret for feilen og eventuelle følgefeil for denne.

[4] Service Level Agreement

7 Bestilling og leveranse

7.1 Bestilling

7.1.1 Oppstartsmøte

GlobalConnect koordinerer oppstartsmøte med kunden hvor det enes om regelsettet som skal defineres i kundens brannmur.

7.1.2 Bestilling

Bestilling av Nettsentrisk sikkerhetstjeneste gjøres gjennom kundeansvarlig selger. Skjema med teknisk informasjon og kontaktpersoner fylles ut og sendes inn sammen med bestilling av tjeneste.

7.1.3 Endringsforespørsler

Ved endret sikkerhetspolicy i virksomheten eller bruk av nye applikasjoner kan det være behov for å åpne og/eller stenge for trafikk mellom kundens interne nett og Internett.

GlobalConnect har ansvar for all endringshåndtering på den *Nettsentriske brannmuren* og gjennomfører disse i henhold til bestilling fra kunden. I de fleste tilfeller er det kun mindre endringer i regelsettet på brannmuren som raskt kan effektueres. Mer sjeldent er det behov for omfattende endringer hvor kompleksiteten krever mer planlegging.

Endringer på den Nettsentriske brannmuren koordineres med kunden og endringer faktureres per påbegynte time. Endring på den Nettsentrisk Brannmuren utføres kun på oppdrag fra autorisert person hos kunden.

I forbindelse med leveranse, implementering og konfigurasjon av den Nettsentriske brannmuren er det behov for en informasjon relatert til Kundens sikkerhetspolicy og regelsett.

Oppdrag vil normalt påbegynnes innen påfølgende virkedag etter mottatt bestilling og avtales i hvert enkelt tilfelle med kunden.

7.2 Leveranse

7.2.1 IPVPN-kunder

For IPVPN-kunder tilpasses regelsettet som gjenspeiler kundens sikkerhetspolicy. Før implementasjon av tjenesten fylles et eget teknisk bestillingskjema ut av kunden i samarbeid med teknisk salgsstøtte hos GlobalConnect.

7.2.2 Teknisk kontaktperson

I forbindelse med oppsett av tjenesten er dialog nødvending mellom kundens tekniske kontaktperson (autorisert kontaktperson hos kunden) og GlobalConnect. GlobalConnect må informeres om teknisk kontaktperson og autorisert bestiller hos kunde.

7.2.3 GlobalConnect Security Operations Center (SOC)

GlobalConnect Security Operations Center leverer *sikkerhet som en tjeneste* og utfører implementasjon, drift og vedlikehold av sikkerhetstjenestene.

8 Appendix 1, URL kategorier

Abortion	Parked
Abused Drugs	Peer – to Peer
Adult	Personal Sites and Blogs
Alcohol and Tobacco	Philosophy and Political Advocacy
Auctions	Phirsing
Business and Economy	Private IP Addresses
Computer and Internet Info	Proxy Avoidance and Anonymizers
Content Delivery Networks	Questionable
Dating	Real Estate
Educational Institutions	Recreation and Hobbies
Entertainment and Arts	Reference and Research
Financial Services	Relgion
Gambling	Search Engines
Games	Sex Education
Government	Shareware and Freeware
Hacking	Shopping
Health and Medicine	Social Networking
Home and Garden	Society
Hunting and Fishing	Sports
Internet Portals	Stock Advice and Tools
Job Search	Streaming Media
Legal	Swimsuits and Intimate Apparel
Malware	Training and Tool
Military	Transaltion
Motor Vehicles	Travel
Music	Weapons
News	Web Advertisements
Nudity	Web Hosting
Online Storage and Backup	Web-based Email