Dienstbeschrijving SURFfirewall

Juli 2021

Auteur(s): Richa Malhotra, Nils Vogels, Eyle Brinkhuis
Versie: 0.951
Datum: 30/07/2021
Kenmerk: Dienstbeschrijving voor de dienst SURFfirewall

Inhoudsopgave

1 Inleiding

Deze dienstbeschrijving beschrijft de dienst SURFfirewall-*Basic*. Dit document is bedoeld voor de Coördinerend SURF Contactpersoon (CSC), Instellingscontactpersoon (ICP), de Instellingscoördinator (ICO) en eventueel andere personen binnen de instelling die betrokken zijn bij het leveren van ICT-dienstverlening.

In dit document komen achtereenvolgens aan de orde:

1. Beschrijving van de dienst;
2. Beschrijving van de dienstverlening;
3. Garanties van beschikbaarheid en betrouwbaarheid;
4. Contactgegevens en informatie over aanvraag, wijziging en storingsprocedures.

1.1 Soort dienst

SURFfirewall-*Basic* biedt firewall capaciteit en functionaliteit aan instellingen. SURFfirewall "Basic" kan gezien worden als aanvullende dienst bovenop SURFinternet maar kan ook gezien worden als vervanging van een externe(perimeter) firewall bij de instellingen.

SURF opereert een redundante Firewall cluster als basis voor deze dienst en regelt de integratie met SURFinternet. Daarnaast worden er beheersdiensten en expertise ingekocht.

1.2 De rol van SURF

SURF heeft een centrale rol in de operatie van de Firewall dienstverlening, treedt op als service provider voor beschermde internetverbindingen. Daarnaast begeleidt SURF, middels een partner, de volwassenwording van het beveiligingsbeleid en uitvoering daarvan bij deelnemende instellingen. SURF leidt ook toekomstige ontwikkelingen (zie 2.1.2) van de dienst in samenspraak met de instellingen.

2 Beschrijving SURFfirewall

2.1 Achtergrond

Bij een SURF relatiedag is SURFfirewall uitgeroepen tot een dienst die SURF zou moeten ontwikkelen. Vlak daarna is SURF begonnen met een behoeftepeiling om te begrijpen hoe zo'n dienst eruit zou moeten zien. Er zijn een aantal interviews gedaan en er bleek dat er behoefte was voor 2 varianten van een SURFfirewall dienst: *Basic* en *Managed*.

Een instelling die graag alles uitbesteedt, heeft het liefst een Firewall waarbij de verantwoordelijkheid voor beheer, security-advies en een vertaling daarvan in uitvoering bij SURF ligt. Hier is er een behoefte aan een *Managed Firewall*.

Instellingen die open staan voor uitbesteding, maar niet per se een duidelijke strategie hiervoor hebben, bepalen meestal per-case of ze een dienst van SURF (of een marktpartij) afnemen. De Firewall-dienst moet dan voldoende toegevoegde waarde bieden en zou niet duurder moeten zijn dan hun huidige oplossing. De toegevoegde waarde zien ze in beheer en het flexibel kunnen opschalen van capaciteit en functionaliteit. Ook willen ze security-advies van SURF, maar wel zelf de regie houden op de security policies en de uitvoering daarvan. Ze zeggen: "We krijgen veel securityadvies van marktpartijen maar weten niet of we ze kunnen vertrouwen". Wat betreft policy willen deze instellingen zelf aan het roer staan, want er zitten veel afhankelijkheden met hun interne netwerk, diensten en applicaties waar SURF op dit moment geen rol in speelt. Een *Basic Firewall*, een 'first line of defense', kan hier een oplossing bieden. Een andere zinvol use-case, is de wens om een deel van de functionaliteit of capaciteit van een instellingsfirewall te off-loaden naar een Firewall van SURF.

Kwantitatief onderzoek binnen de MBO en HBO sectoren (waar meeste interesse blijkt te zijn) ondersteunde de behoefte aan een Basic en Managed variant van een Firewall dienst. Hierna is een pilot uitgevoerd samen met een aantal instellingen om de technische werking van deze dienst te testen. Na de pilot is gebleken dat op dit moment de "Basic" firewall de meeste haalbare en kansrijke variant is. Daarom heeft SURF besloten om allereerst deze SURFfirewall-*Basic* in productie te brengen. Dit document beschrijft deze dienst.

2.1.1 Propositie

Met SURFfirewall hoeft de instelling zich geen zorgen meer te maken over de rechtmatigheid van de inkoop van hun firewall. De instelling hoeft geen aanschaf meer te doen die tot het einde van de afschrijftermijn gebruikt kan worden, wat inefficiëntie in de hand werkt. De SURFfirewall oplossing kan namelijk (binnen vastgestelde kaders) meeschalen met de behoefte van de instelling. De instelling hoeft geen kennis meer te onderhouden van specifieke firewalltechnieken, maar kan zich focussen op het vaststellen van (security) beleid en andere zaken die hen onderscheiden.

SURFfirewall-*Basic* biedt de volgende voordelen voor de instellingen:

- geen aanbestedingslast voor hardware en/of software/licenties
- geen beheerslast voor hardware en/of software
- geen configuratielast
- minder kennis nodig in-house
- flexibel opschalen en afschalen in capaciteit en daardoor beter aansluiten met de actuele capaciteitsbehoefte
- mogelijk kostenvoordeel door betere match tussen gekochte en gebruikte

functionaliteit/capaciteit en centrale inkoop
- volledig integratie met SURFinternet

De dienst kan worden gezien als een verlengde van SURFinternet door sommige instellingen of als vervanging van hun externe /perimeter firewall. SURFfirewall-*Basic* is een aparte SURF dienst met zijn eigen tariefmodel. Door SURFfirewall-*Basic* af te nemen kunnen instellingen zich beter focussen op de (security) beleid en andere zaken die hen onderscheiden.

2.1.2 Toekomstvisie

Tijdens de gesprekken met de instellingen zijn veel wensen naar voren gekomen. Op basis van deze wensen en technologische ontwikkelingen is een toekomstvisie en roadmap geformuleerd voor SURFfirewall.

Op de ***middellange termijn*** zal SURF een SURFfirewall-*managed* ontwikkelen en proactief advies leveren. Hiermee bestaat de mogelijkheid om in community verband samen met collega instellingen gestandaardiseerde security policies te ontwikkelen. Hierin kan aandacht worden besteed aan makkelijker uitwisseling van (onderzoeks)data tussen instellingen of verschillende beleid voor verschillende soorten verkeer en dit op een uniforme manier toepassen in SURFfirewall. Sommige instellingen hebben de wens uitgesproken om hun interne firewalls ook bij SURF neer te leggen. De SURFfirewall-Basic zal dan ook verder ontwikkeld woorden om deze functionaliteit te bieden. Verder zal ook gewerkt worden aan integratie met SURFsoc.

Op de ***lange termijn*** verwachten we dat door digitalisering er veel meer data gegenereerd zal worden voor onderwijs en onderzoek die naast op de campus ook in meerdere clouds en externe data-centers opgeslagen zal worden. Dan hebben we het niet meer over 1 fysieke campus maar een virtueel campus dat verspreid is omdat de data van de campus op veel plekken zich zal manifesteren. Deze data moet ook op alle plekken beveiligd worden. Daardoor zal een behoefte ontstaan voor Firewalls en security mechanismen op meerdere plekken die heel snel geregeld kunnen worden met een "Firewall-on-demand", binnen uren/minuten. Daarnaast willen de instellingen het liefst betalen voor het echte gebruik "Pay-per-use" want als je de data verwijderd van een locatie wil je ook van de Firewall en andere security mechanisms op die locatie af. Verder, wil een instelling het liefst dan ook de hele "virtual" campus en de bijbehorende firewalls en de data op verschillende locaties kunnen beheren via 1 ingang (bijv. een portaal).

Onze ambitie is te kunnen voldoen aan deze toekomstige behoeftes van de instellingen en dit is ook de visie van deze dienst. Met uitbreiding van het SURF netwerk (op veel meer locaties en clouds), gebruik van NFV technologie en ontwikkelen van portalen kunnen we deze ambitie waarmaken en het business model verder ontwikkelen in de toekomst.

2.2 Functionele beschrijving van de dienst

2.2.1 Samenvatting

Met de SURFfirewall-*Basic* dienst biedt SURF deelnemende instellingen de mogelijkheid om de SURFinternet verbinding te beveiligen met een moderne next-generation Firewall. De beschikbaarheid en het functioneren van deze firewall wordt geheel uit handen genomen en instellingen hoeven zich alleen nog bezig te houden met de uitvoering van het beveiligingsbeleid (de firewallregels) en niet meer de inkoop, het onderhoud en schaling van hun firewall. Het is momenteel mogelijk om maximaal 5 virtual LANs (VLANs) of security zones (binnen instellingsnetwerk) te laten filteren door SURFfirewall.

Met SURFfirewall-*Basic* kunnen deelnemende instellingen de inkoop- en beheerslast van een firewall bij SURF neerleggen. Instellingen nemen een Firewall op maat af, passend bij hun beveiligings- en verkeersbehoefte.

	Inkoop **Hardware en licenties**	**Beheer** **hardware**	**Inrichting en beheer software**	**Firewall** **configuratie**	**Policies**
SURFfirewall *Basic*	SURF	SURF	SURF	SURF	Instelling

De **SURFfirewall-*Basic*** zal geleverd worden met volledig gelicenseerde (UTM, Unified Threat Management) functionaliteit van een FortiGate, een firewall van Fortinet. Dit is de maximale belasting voor een firewall en daarom minimaal haalbare doorvoersnelheid. SURF regelt hardware inkoop, beheer, licenties en integratie met SURFinternet. Instelling krijgt een interface om zelf firewall regels in te voeren en te beheren, de beheersportaal.

2.2.2 Voor bestuurders

SURF neemt de uitvoering van de beveiliging uit handen. Uw ICT medewerkers voeren het beveiligingsbeleid in, SURF draagt zorg voor de uitvoering.

2.2.3 Voor ICT managers en beheerders bij instellingen

Door een firewall bij SURF af te nemen, wordt deze automatisch geïntegreerd in de SURFinternet verbinding. Een tijdrovend installatietraject is niet nodig, de SURFinternet verbinding wordt na activeren van SURFfirewall-*Basic* beveiligd opgeleverd. De capaciteit van de SURFfirewall kan meeschalen met de groeiende behoefte van de instellingen. Er zal een nieuwe verbinding worden opgeleverd met daarin de SURFfirewall actief op een al bestaande service poort, zodat migratie op jullie tempo plaats kan vinden. De instelling blijft verantwoordelijk voor de Firewall regels/security beleid en de keuzes die daarin worden gemaakt.

2.3 Technische inrichting van de dienst

Deze sectie beschrijft hoe de dienst technisch is ingericht.

2.3.1 Virtuele domeinen

Binnen het firewall cluster wordt voor iedere instelling een virtueel domein aangemaakt. Dit virtuele domein bevat de firewall en de beveiligingsregels en specifieke instellingen. Door gebruik te maken van virtuele domeinen is het zowel mogelijk om meerdere firewalls per instelling in te richten, als om per firewall meerdere instellingen aan te koppelen.

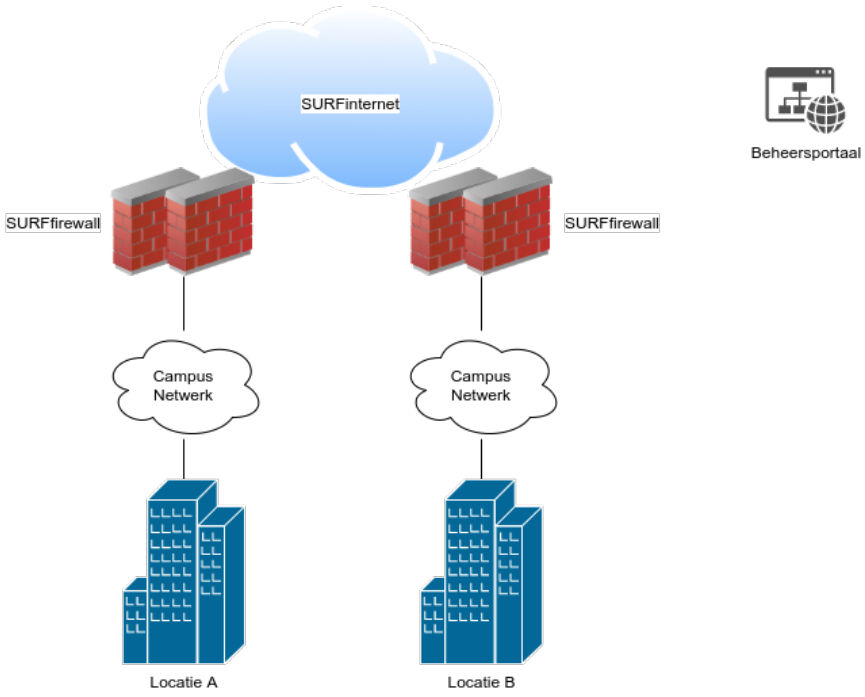
Door het maximale verkeer wat door zo'n virtueel domein gaat te beperken op wat de instelling afneemt, wordt bovendien het risico op overbelasting bij een eventuele aanval verminderd.

2.3.2 Integratie met SURFinternet

De SURFfirewall-Basic dient als 'edge' of 'border' firewall, en ontsluit de instelling op een of meerdere locaties aan SURFinternet. Voor de instelling is de SURFfirewall het nieuwe

koppelpunt geworden met het SURF netwerk: In plaats van met de SURF routers koppel je met de SURFfirewall middels BGP of eventueel statische routering.

De SURFfirewall dienst is redundant opgezet, waardoor je altijd meerdere firewalls hebt en meerdere netwerkpaden, om eventuele verstoringen op te vangen.



2.3.3 Beveiligd beheer

Alleen geautoriseerde beheerders van de instelling hebben toegang tot de beheersportaal.
Op het beheersportaal kun je inzicht krijgen in de huidge staat van de firewall, en de het firewall-beleid (de “rulebase”) veranderen, en deze actief maken op jullie firewall.

De autorisatie voor de beheersportaal wordt gedaan door gebruik te maken van SURFconext. Zo zijn wij er zeker van dat alleen de gebruikers die vanuit de instelling toegang behoren te hebben, ook daadwerkelijk toegang krijgen.

Wij zullen bij aanvragen van de eerste firewall bij een instelling contact opnemen met bij ons reeds bekende contactpersonen, om zo de eerste beheerder te bepalen. Hierbij nemen wij contact op met de ICP’s en SURFcert contactpersonen. Verdere beheerders worden door de eerste beheerder aangedragen. Mocht de eerste beheerder niet meer in dienst zijn, nemen wij weer contact op met de ICP’s en SURFcert contactpersonen.

Als een beheerder niet meer werkzaam is bij een instelling, is het de verantwoordelijkheid van de instelling om dit aan SURF door te geven. Wij zullen het beheerdersprofiel conform ons privacybeleid verwijderen. Natuurlijk werkt de toegang voor de beheerder niet meer zodra er middels SURFconext niet meer kan worden geauthenticeerd.

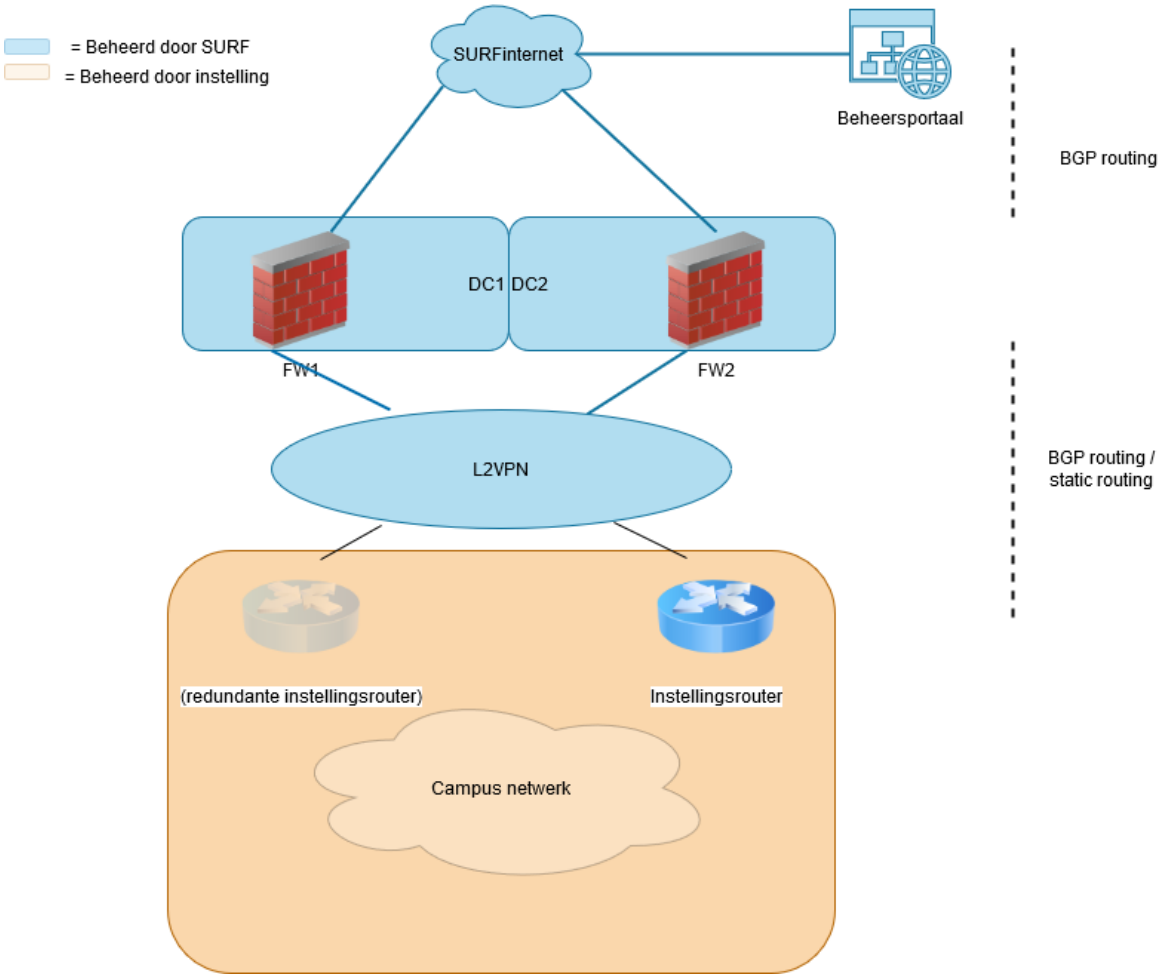
2.3.4 Next Generation Firewall

Zoals eerder genoemd zal de SURFfirewall geleverd worden met volledig gelicenseerde (UTM, Unified Threat Management) functionaliteit. Onder “Unified Thread Management” vallen diverse Next Generation firewall functionaliteiten, zoals:

- Antivirus
- Botnet detection
- IP/Domain Reputation
- IPS
- NGFW (Next Generation Firewall) Application Control
- Virus Outbreak Protection
- Web Filtering

Hiermee is het mogelijk om op basis van applicaties, of zelfs inhoud van verkeer beveiligingsbeleid op te stellen en af te dwingen.

2.3.5 Opbouw van de connectiviteit



De dienst is opgebouwd uit een drietal delen:

1. Een reguliere, redundante, SURFinternet verbinding, met daarop de DDoS filters aangeschakeld op standaard waarden
2. Een hoog-beschikbare firewall die middels BGP gekoppeld is aan de SURF routers
3. Een L2VPN, waarin de firewall redundant is gekoppeld, samen met de aangewezen SURF poorten van de instelling, waarbij de dienst wordt geleverd als VLAN op deze poort (max 5 VLANs).

2.4 Technische aansluiting van de dienst

Deze sectie beschrijft de aspecten waar de instellingen mee te maken zullen krijgen bij het aansluiten van de SURFfirewall-*Basic* met hun (campus) netwerk.

2.4.1 Schaalbare bandbreedte

De capaciteit van de firewall die de instellingen afnemen kan het beste bepaald worden door de grootte van het verkeersaanbod op hun SURFinternet verbinding. SURF adviseert on naar het werkelijke verkeer te kijken en niet naar de aansluitsnelheid van de SURFinternet aansluiting. Hierdoor betalen de instellingen niet meer dan nodig is om de aansluitingen te beveiligen. Het is bijvoorbeeld mogelijk om je 10Gbit/s internetverbinding te voorzien van een 2Gbit/s firewall, omdat je instelling hier voldoende aan heeft. Dit scheelt maandelijks in de kosten van de firewall.

2.4.2 Koppeling SURFfirewall

Bij aanvragen van een SURFfirewall wordt deze doorgaans als een 2e verbinding opgeleverd, zodat migratie van het internetverkeer geleidelijk plaats kan vinden. Onze ervaring leert dat tijdens migratie er altijd snel firewall wijzigingen moeten worden doorgevoerd omdat er onbedoeld verkeersstromen onderbroken worden. Natuurlijk is het in overleg mogelijk om de SURFfirewall direct alle verkeersstromen af te laten handelen.

De firewall kan worden aangekoppeld met BGP (dit heeft onze voorkeur) of als statische routering. Bij statische routering is het niet mogelijk om zonder betrokkenheid van SURF het verkeer te sturen tussen meerdere aansluitingen, of om de routing van de firewall naar het campusnetwerk te veranderen

2.4.3 Aansluittraject

Bij het afnemen van deze dienst hoort een aansluittraject. In het verleden hebben wij gemerkt dat namelijk geen enkele netwerkomgeving hetzelfde is, en de meeste omgevingen even moeten worden doorgesproken om het gebruik van deze dienst soepel te laten verlopen.

In dit aansluittraject zal met de deelnemer worden besproken:

– De algemene technische eigenschappen van SURFfirewall-*Basic*. De specifieke zaken van de netwerkomgeving van de afnemende instelling
– Details over de netwerkkoppelingen tussen de deelnemer en de SURFfirewall -*Basic* dienst
– Details over het beveiligingsbeleid van de deelnemer tbv de SURFfirewall dienst
-- Een stappenplan om te komen tot aansluiting

Naar aanleiding van het aansluittraject zal een situatietekening worden gemaakt voor de deelnemer, die ter beschikking komt van de SURF Helpdesk ten behoeve van het spoedig verhelpen van mogelijke verstoringen. Hierbij wordt er niet zelden gekozen om slechts een gedeelte van het totale verkeer door de firewall te leiden, om zo de dienst efficiënter af te kunnen nemen. Omdat de dienst als aparte internetverbinding wordt geleverd, kan de instelling per IP adres kiezen of het verkeer voor dit IP adres (of reeks) beveiligd moet worden.

3 Dienstverlening

3.1 Gerelateerde diensten

Voor het juist functioneren van SURFfirewall is momenteel een SURFinternet aansluiting nodig.

3.2 Privacy, Security en AVG

Uitgangspunt van deze dienstverlening is dat SURF zorgdraagt voor de netwerkverbindingen en een beveiligd platform wat door de instelling gebruikt kan worden om hun SURFinternet verbinding te voorzien van een beveiligingsbeleid. De inhoud van het beveiligingsbeleid en het instellen van de Firewall om dit juist af te handelen wordt in de “Basic” dienstvariant aan de instelling overgelaten. Voor het opstellen van het beveiligingsbeleid en het instellen van de firewall is eventueel hulp beschikbaar vanuit SURF.

3.2.9 Rechten van betrokkenen

SURF heeft de rol van verwerker bij deze dienst, waar de afnemende instelling verwerkingsverantwoordelijke is. Om deze reden worden betrokkenen aangeraden contact op te nemen met de afnemende instelling om hun rechten uit te oefenen. SURF zal, waar technisch mogelijk, gehoor geven aan verzoeken van de instelling hieromtrent.

3.2.1 Persoonsgegevens

Aangezien de instelling de verantwoordelijkheid heeft voor het opstellen van het beveiligingsbeleid en de instellingen in de firewall, is het bijbehorende privacybeleid ook aan de instelling om op te stellen en na te leven. Hierbij moet worden opgemerkt dat SURF’s normenkaders van toepassing zijn en dat het niet de bedoeling is om zonder zorgvuldige weging deze dienst te gebruiken om de vrijheden op het Internet te beperken.

Daarnaast verwerkt SURF in opdracht van de instelling mogelijk gevoelige gegevens, waarvan een beknopte versie hieronder is weergegeven. In de praktijk kan dit afwijken, indien de instelling de controle heeft over de exacte werking van de firewall (beveiligingsbeleid)

Categorie	Persoonsgegevens	Bijzonder
Studenten	IP-adres, poort, protocol en inhoud van het verkeer ten tijde van internetgebruik	Nee
Instellingsmedewerkers	IP-adres poort, protocol en inhoud van het verkeer ten tijde van internetgebruik	Nee
Beheerder firewall instelling	IP-adres (logging), username, eduPersonTargetedID, uitgevoerde beheershandelingen	Nee
SURF technisch beheerders	Username, IP-adres (logging), thuis IP-adressen, uitgevoerde beheer handelingen	Nee
Externe beheerder	Username, IP-adres (logging), SSH-account, thuis IP-adressen	Nee

De precieze verwerking van persoonsgegevens bij het filteren door de firewall, hangt af van de firewall regels die een afnemende instelling instelt en de persoonsgegevens die daarbij nodig zijn om het verkeer te filteren. De afnemende instelling heeft hier het specifieke inzicht in. Deze regels hebben vooral invloed op de verwerking van persoonsgegeven van gebruikers van het netwerk van de instelling (studenten en instellingsmedewerkers).

Beleidsregels kunnen bestaan uit:

IP reeksen en adressen
Protocol details
Groepslidmaatschappen
Tijdsperiodes
Applicatiesoorten

Aanvullend kunnen op verzoek van afnemers specifieke criteria als beleidsregel op worden genomen, bijvoorbeeld voor herkenning van een specifiek virus of verkeerspatroon. De instelling heeft hier altijd de hulp van SURF voor nodig.

3.2.2 Verwerkingsdoeleinden en belangen

Het is aan de afnemende instelling (verwerkingsverantwoordelijke) om te bepalen voor welke doeleinden persoonsgegevens worden verwerkt en welke persoonsgegevens noodzakelijk zijn voor deze doeleinden. Het is dus aan de afnemende instelling om bij het gebruik van een firewall te bepalen voor welke doeleinden een firewall wordt ingezet en welke persoonsgegevens worden verwerkt voor deze doelen. Het daadwerkelijk uitvoeren van deze verwerkingen vindt dan plaatst binnen de infrastructuur van SURFfirewall.

De volgende algemene doeleinden zijn nu bij SURF bekend:

Beveiliging
Toegangsbeperking
Gegevensbescherming
Opsporen misbruik van het netwerk

De volgende belangen zijn nu bij SURF bekend:

- Het beveiligen van het interne netwerk van de instellingen, doormiddel van firewall-regels. Het gaat hier dus o.a. om het voorkomen van oneigenlijke toegang of misbruik van het door de firewall beschermde netwerk.
- Het optimaal laten functioneren van het netwerk en zorgdragen voor de beschikbaarheid. Bijvoorbeeld door verstorend verkeer op de firewall te blokkeren, voordat het impact heeft op het interne netwerk. Denk hier bijvoorbeeld aan het blokkeren van een DDOS.

3.2.3 Verwerkingen

De gegevensverwerkingen zijn erop gericht om de firewall dienst mogelijk te maken en te kunnen leveren aan de instellingen. Naast de verwerkingen rond de firewall zelf, zijn er ook verwerkingen rond het aanmaken van beheeraccounts, leveren van support, logging en het opstellen van rapportages. Deze worden op verzoek met de afnemende instelling gedeeld.

3.2.4 Verwerkingslocaties

Alle verwerkingen vinden plaats binnen de EER. Het kan zijn dat er voor het juist functioneren van de dienst ondersteuning nodig is van een partij buiten de EER. Deze heeft dan niet direct toegang tot persoonsgegevens. Hierbij valt te denken aan een leverancier van software, welke door subverwerkers kan worden ingeroepen.

3.2.5 Betrokken partijen

SURF onderscheidt bij deze dienst een aantal partijen:

- De afnemende instelling (verwerkingsverantwoordelijke)
- SURF (verwerker)
- Door SURF betrokken beveiligingspartij (subverwerker)

3.2.6 Juridisch en Beleidsmatig kader

Het SURF Juridisch Normenkader (Cloud)services van SURF, de Handreiking Security en het Privacybeleid van SURF zijn van toepassing.

3.2.7 Bewaartermijnen

Op verschillende persoonsgegevens zijn verschillende bewaartermijnen van toepassing. Zo wordt de logging van de acties van een beheerder anders beoordeeld dan de logging van verkeersinspecties. Verkeersinspecties worden na 6 weken verwijderd, terwijl andere persoonsgegevens bewaartermijnen hebben die mogelijk afhankelijk zijn van de duur van de dienstafname. Voor een exacte opgave van bewaartermijnen kunt u met SURF contact opnemen.

3.2.8 Rechten van betrokkenen

SURF heeft de rol van verwerker bij deze dienst, waar de afnemende instelling verwerkingsverantwoordelijke is. Om deze reden worden betrokkenen aangeraden contact op te nemen met de afnemende instelling om hun rechten uit te oefenen. SURF zal, waar technisch mogelijk, gehoor geven aan verzoeken van de instelling hieromtrent.

3.3 Beveiliging

3.3.1 Patching

Regelmatig ontvangt SURF van een betrokken beveiligingsbedrijf het advies rondom het installeren van beveiligingsupdates. Deze patches worden zo snel mogelijk geinstalleerd. Het kan voorkomen dat wij vanwege de urgentie van de beveiligingsupdate buiten reguliere onderhoudsvensters werkzaamheden moeten verrichten. Deze werkzaamheden worden nogsteeds vooraf aangekondigd, en waar nodig dezelfde dag geinstalleerd. Voor een afweging van het spoedeisende karakter wordt de CVSS 2.0 index gebruikt.

Hierbij moet wel opgemerkt worden dat uiteindelijk de instelling verantwoordelijk is voor het voeren van een beveiligingsbeleid en het juist afstemmen van de SURFfirewall configuratie op dit beleid.

3.3.2 Role based access

Alle vormen van toegang zijn onderworpen aan role-based access control, waarbij de standaard rol geen toegang oplevert. Op deze manier zorgen wij voor het verlenen van de minst mogelijke toegang om de werkzaamheden uit te kunnen voeren

3.3.3 Hardening

Op de firewalls zelf staan alle onnodige functionaliteiten uit. Dit wil zeggen dat wij een functie pas inschakelen op het moment dat hier noodzaak voor is. Op deze manier voorkomen wij het onnodig misbruik van functies van de firewall

3.3.4 Versleuteling

Alle communicatie met de firewall gebeurt versleuteld middels daarvoor geldende standaarden (TLS1.3). Alle opslag op firewall hardware gebeurt versleuteld.

3.4 Audits vanuit SURF

De kwaliteit en veiligheid van de dienstverlening is voor SURF belangrijk. Daarom worden er de volgende audits uitgevoerd:

Onderdeel	Soort audit	Frequentie
Alle publieke interfaces van de dienst	Pentest (blackbox)	Jaarlijks
De complete infrastructuur	Pentest (whitebox)	Eens per 3 jaar
Processen en procedures	Administratief	Volgens programma SURF

3.5 Rollen en verantwoordelijkheden

Om de dienst volgens verwachting te laten werken, is het belangrijk een overzicht te geven van de rollen en verantwoordelijkheden zoals deze bij het ontwerp is vastgelegd.

Rol	Verantwoordelijkheid	Toebedeeld aan
Operationeel beheerder	Het werkend houden van de firewall	SURF (uitbesteed aan 3e partij)
Netwerk integratie non-campus	Het integreren van de firewall met het netwerk	SURF
Netwerk integratie campus	Het integreren van de firewall met het campus netwerk	Instelling
Beveiligingsbeheer	De firewall voorzien van de juiste beveiligingsregels	Instelling
Toegangsbeheer	Toegang tot de beheersportaal beperken	SURF
Verwerker	In de zin van de AVG	SURF
Verwerkingsverantwoordelijke	In de zin van de AVG	Instelling
Subverwerker	In de zin van de AVG	3e partij

3.6 Serviceniveaus

Bij de “Basic” variant zorgt SURF voor de technische infrastructuur buiten het netwerk van de

Instelling: We stellen een verbinding beschikbaar op een al bestaande service poort van de instelling, en verzorgen vanaf hier de beveiliging en de internet verbinding. SURF zorgt ervoor dat de omgeving beschikbaar en bijgewerkt blijft en laat de omgeving regelmatig door een beveiligingsbureau testen.

Bij de beveiliging van het netwerk van de instelling wordt er vanuit gegaan dat de instelling hiervoor correcte beveiligingsregels opstelt middels de Firewall beheersportaal.

Op maandelijkse basis levert SURF rapportage rondom het algemene functioneren van de firewall, die via E-mail zullen worden toegestuurd. Hierbij valt te denken aan de belasting van de firewall, maar ook de meest waargenomen bedreigingen op de internetverbinding van de instelling.

Voor specifieke serviceniveaus verwijzen we verder naar de SLS parameters in paragraaf 4.3 van deze dienst.

Op termijn zal een “Managed” variant beschikbaar komen met een tweede service niveau. Deze variant is nog in ontwikkeling. Op het moment dat deze beschikbaar komt, kunnen deelnemers een upgrade uitvoeren, zonder dat hier onderhoud op de dienst voor nodig is.

3.7 Tarieven

De meest recente tariefinformatie is terug te vinden in de jaarlijkse tarievenbrief of via Klantsupport@surf.nl.

De tarieven kennen een eenmalige, vaste en flexibele component.

SURFfirewall “Basic”
Alle firewalls worden initieel geleverd met volledig gelicenseerde Next Generation of Unified Threat Management(UTM) functionaliteit. Dit is de maximale belasting voor een firewall en daarom minimaal haalbare doorvoersnelheid.
SURF regelt hardware inkoop, beheer, licenties en integratie met SURFinternet. Instelling krijgt een interface om zelf firewall regels in te voeren en te beheren

3.8 Andere voorwaarden en bepalingen

3.8.1 Beveiligingsmaatregelen

De instelling moet zelf beveiligingsmaatregelen nemen en niet alleen op de beveiliging van SURFfirewall steunen.

3.8.2 Duur en Beëindiging

Indien de overeenkomst tussen SURF en de door haar gecontracteerde leverancier(s) van hard- en software wordt beëindigd zal SURF de instellingen op de hoogte brengen en op zoek gaan naar een alternatieve oplossing. In het geval dat geen structurele vervangende oplossing geregeld kan worden hanteert SURF een overgangsperiode van 3 maanden met de instelling. Tijdens de overgangsperiode wordt verwacht dat de instelling overstapt naar een alternatieve oplossing.

4 Garanties, rapportages en beschikbaarheid

4.1 Garanties

De algemene bepalingen zoals geformuleerd in de SURFnet Service Level Specificatie (https://www.surf.nl/files/2021-07/surfnet-service-level-specificatie-14.0.pdf) zijn op SURFfirewall van toepassing. De meest recente versie van de SLS is te vinden op https://wiki.surfnet.nl/display/SURFnetnetwerkWiki/SURFfirewall .

4.2 Rapportages

Rapportage over de karakteristieken van SURFfirewall-*Basic* publiceren we op SURFdashboard. Dienst specifieke statistieken, logging, troubleshooting informatie en rapportages stellen we via specifieke SURFfirewall-*Basic* rapportages aan de instelling beschikbaar.

4.3 Beschikbaarheid

Voor SURFfirewall-*Basic* gelden de volgende beschikbaarheidspercentages:

Beschikbaarheid component	Waarde op jaarbasis
Beschikbaarheid netwerkverbinding	99,9%
Beschikbaarheid beheersportaal	99,5%

5 Vragen, aanvragen, wijzigingen en storingen

5.1 Vragen

Algemene vragen over de dienst kunnen gesteld worden via SURFfirewall-beheer@surf.nl

5.2 Aanvragen, wijzigen, opzeggen

SURFfirewall is beschikbaar voor op SURFinternet aangesloten instellingen. Voor een aanvraag of wijziging kan de instellingscontactpersoon (ICP) terecht bij SURF Klantsupport.

SURF Klantsupport (kantooruren):	+31 88 7873 000 Klantsupport@surf.nl

5.3 Storingen

In geval van een storing kan de daarvoor bevoegde persoon zich melden bij de Helpdesk.

SURF Helpdesk (24/7):	088 – SURFNET (088 7873 638)