Samen aanjagen van vernieuwing

Bijlage 1 Opdrachtomschrijving dienst SURFfirewall

Inhoudsopgave

Inhoud

Omschrijving dienst SURFfirewall

Soort dienst

SURFfirewall biedt firewall capaciteit en functionaliteit aan instellingen. SURFfirewall kan gezien worden als aanvullende dienst bovenop de SURFinternet dienstverlening, maar kan ook gezien worden als vervanging van een externe(perimeter) firewall bij de instellingen. SURF opereert een geografisch gescheiden, redundant Firewall cluster als basis voor deze dienst en regelt de integratie met SURFinternet. Daarnaast worden beheerdiensten en expertise ingekocht en wordt voorzien in logging en analyse-mogelijkheden op basis van de firewall-configuratie.

Rol van SURF

SURF heeft een centrale rol in de operatie van de firewall dienstverlening en treedt op als serviceprovider voor beschermde internetverbindingen. Daarnaast begeleidt SURF, middels een partner, de volwassenwording van het beveiligingsbeleid en uitvoering daarvan bij deelnemende instellingen. SURF leidt toekomstige ontwikkelingen van de dienst in samenspraak met de instellingen.

Beschrijving SURFfirewall

Achtergrond

Bij een SURF relatiedag in 2018 hebben de aanwezige instellingen aangegeven dat SURFfirewall een dienst is, die door SURF ontwikkelt zou moeten worden. Daarna is SURF begonnen met een behoeftepeiling om te begrijpen hoe deze dienst eruit zou moeten zien. Er zijn verschillende interviews gedaan en er bleek dat er behoefte was voor twee 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 implementatie daarvan in uitvoering bij SURF ligt. Hier is er een behoefte aan een *Managed Firewall*.

Instellingen die open staan voor uitbesteding en bepalen daarin, meestal per-case, of ze een dienst van SURF afnemen. De SURFfirewall-dienst moet 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. 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 zinvolle use-case is de wens om een deel van de functionaliteit of capaciteit van een instellingsfirewall te offloaden naar een firewall van SURF.

Vanwege de complexiteit in rollen en verantwoordelijkheden die SURFfirewall-Managed met zich meebrengt is besloten de ontwikkeling van deze Managed variant in een later stadium te starten.

Functionele beschrijving van de dienst

Met de SURFfirewall-*Basic* dienst biedt SURF deelnemende instellingen de mogelijkheid om de SURFinternetverbinding te beveiligen met een moderne next-generation firewall. De beschikbaarheid en het functioneren van deze firewall wordt geheel uit handen genomen. Instellingen hoeven zich alleen bezig te houden met de uitvoering van het beveiligingsbeleid en niet meer de inkoop, het onderhoud en de schaling van deze firewall.

Met SURFfirewall-*Basic* kunnen deelnemende instellingen de inkoop- en beheerlast van een firewall bij SURF neerleggen. Instellingen nemen een firewall op maat af, passend bij hun beveiligings- en verkeersbehoefte, in stappen van 1Gbit/s UTM-capaciteit.

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

De SURFfirewall-*Basic* variant wordt geleverd met volledig gelicenseerde (UTM, Unified Threat Management) functionaliteit. Deze functionaliteit is vanaf dag 1 actief. SURF zorgt voor de hardware inkoop, beheer, licenties en integratie met SURFinternet of andere externe connectiviteit. Instellingen beschikken over een (web)interface om zelf de configuratie (firewall regels) te beheren.

Tevens is voor de afnemende instellingen een logging- en analysetool beschikbaar, om inzicht te krijgen in de verkeerskarakteristieken en/of threats.

Technische inrichting van de dienst

Deze paragraaf beschrijft hoe de dienst technisch is ingericht.

Systeemslices

Binnen het firewall cluster wordt voor iedere instelling een systeemslice aangemaakt. Dit virtuele domein bevat de firewall, beveiligingsregels en specifieke configuratie zoals BGP, IPsec of SSL VPN voor iedere instelling. Door gebruik te maken van virtuele domeinen is het zowel mogelijk om meerdere firewalls per instelling in te richten, alsmede per firewall meerdere instellingen te koppelen. Een bijkomend voordeel is het efficiënt gebruiken van de firewallcapaciteit. Zo passen er meerdere instellingen op een fysiek firewall-cluster. De hardware wordt gesliced op basis van de beschikbare NGFW-capaciteit. De capaciteit wordt per Gigabit/s NGFW per maand aangeboden. Logging die wordt gegenereerd door de firewallinstantie wordt voor een maximum van 58 dagen bewaard en beschikbaar gesteld voor analyse.

Beveiligd beheer

Alleen geautoriseerde beheerders van de instelling hebben toegang tot de centrale, web-based beheer- en analyseportaal.

In het beheer- en analyseportaal krijgen de beheerders inzicht in de huidige staat van de firewall, kunnen zij het firewall-beleid veranderen en de configuratie actief maken op hun firewall.

De authenticatie en autorisatie voor het beheer- en analyseportaal wordt gedaan door gebruik te maken van SURFconext, een op SAML2.0 gebaseerde authenticatie en autorisatie-infrastructuur. Zo zijn wij er zeker van dat alleen gebruikers die vanuit de instelling toegang behoren te hebben, ook daadwerkelijk toegang krijgen.

Next Generation Firewall

SURFfirewall wordt geleverd met volledig gelicenseerde (NGFW) functionaliteit. Hieronder 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.

Redundantie

SURFfirewall wordt gerealiseerd op een redundant paar firewalls in active-standby setup. Deze firewalls zijn geografisch gescheiden maar onderling verbonden alsof ze naast elkaar staan. Een Active-Active setup is niet wenselijk vanwege capaciteitsgarantie die wordt afgegeven en de onderliggende transportmechanieken in het SURF-netwerk.

Blueprint

SURF biedt SURFfirewall aan op generiek geconfigureerde firewallclusters. Dat betekent dat de firewall-clusters productierijp gemaakt worden aan de hand van een vooraf gedefinieerde blueprint waarin zaken als redundantie, monitoring, authenticatie & authorisatie, patching, (upstream-) connectiviteit. Dit vereenvoudigt het beheer doordat alle firewall-clusters eenzelfde configuratie genieten.

Toekomst in de techniek

De huidige technische oplossing voor SURFfirewall biedt de mogelijkheid om fysieke firewall-chassis' op te splitsen in meerdere domeinen om zo efficiënt om te gaan met beschikbare capaciteit. SURF werkt hard aan het bouwen en opereren van een Netwerkfunctie Virtualisatie (NFV)-infrastructuur: een private cloud specifiek gebouwd voor hoge doorvoer, lage latency netwerkverkeer. SURF is van mening dat de toekomst voor SURFfirewall op deze NFV-infrastructuur is en werkt daarom aan het beschikbaar stellen van virtuele firewalls op dit KVM/QEMU platform met geaccelereerde netwerk hardware. Dit betekent ook dat de virtuele firewalls moeten beschikken over dezelfde functionaliteiten als de fysieke firewalls.

Om schaalbaar en kosten-efficiënt virtuele firewalls te creëren wil SURF gebruik maken van 'metered' dienstverlening: aan de hand van het verbruik (bijvoorbeeld doorvoersnelheid en/of gebruikte inspectie functionaliteit) wordt maandelijks de factuur opgemaakt per virtuele firewall. Het kostenplaatje moet vooraf inzichtelijk zijn voor een instelling.

Het doel om SURFfirewall virtueel te leveren betekent dat de centrale managementsysteem om moet kunnen gaan met zowel fysieke als virtuele firewalls. Daarmee behouden we één centrale dienstingang voor SURFfirewall. Deze beheer- en logging-omgeving staat bij SURF on-premise vanwege AVG-overwegingen. Het is voor SURF een doel om op termijn louter virtuele SURFfirewall-instanties te leveren aan instellingen.

SURF gebruikt voor het bouwen en leveren van dienstverlening automatiserings- en orkestratie tooling. SURFfirewall is één van de diensten die geautomatiseerd is. Om te kunnen integreren met onze huidige orkestratie en automatiseringsplatform moet de centrale beheeromgeving volledig via een API te besturen zijn, van het aanmaken van systeem-slices tot het configureren van de regelbasis.

Indicatie omvang Instellingen

Onderstaand is een indicatie gegeven van de omvang van verschillende Instellingen. Dit betreft de totale omvang van zo'n Instelling. Indien een Instelling gebruik gaat maken van de firewall-dienstverlening, dan is het zeer wel denkbaar dat niet direct de hele infrastructuur van de Instelling ontsloten wordt naar de firewall. Er kan gekozen worden om slechts enkele delen van het netwerk te ontsluiten via de firewall. De indicatie van de omvang is dan ook bedoeld om een overall beeld te geven van de omvang van een Instelling.

Indicatie omvang omgeving universiteit

Verschillende universiteiten kunnen onderling verschillen in complexiteit en omvang van hun infrastructuur. Een en ander is uiteraard erg afhankelijk van de inrichting van het lokale netwerk en hoe de firewall wordt ingericht en met welke functionaliteit.

Aantal users:

- +/- 25.000 studenten
- +/- 10.000 medewerkers

Indicatie verkeer:

- +/- 15.000 Mbps piek netwerkverkeer door netwerksensoren
- +/- 50.000 concurrent ip-systemen op het netwerk (zowel gast als managed), waarvan:
    - +/- 4.000 servers
    - +/- 15.000 werkplekken
    - Rest BYOD

Indicatie omvang omgeving hogeschool

Onderstaande indicatie is gebaseerd op cijfers van enkele gemiddelde HBO-instelling en een grotere HBO-instelling.

<u>Gemiddelde HBO-instelling:</u>

Aantal users:

- +/- 11.000 studenten
- +/- 1.100 medewerkers

Indicatie verkeer:

- +/- 5.000 Mbps piek netwerkverkeer door netwerksensoren
- +/- 5.000 concurrent ip-systemen op het netwerk (zowel gast als managed), waarvan:
    - +/- 150 servers
    - +/- 1.000 werkplekken
    - Rest BYOD

<u>Grote HBO-instelling:</u>

Aantal users:

- +/- 60.000 studenten
- +/- 6.500 medewerkers

Indicatie verkeer:

- +/- 10.000 concurrent ip-systemen op het netwerk (zowel gast als managed), waarvan:
    - +/- 93 fysieke servers
    - +/- 638 virtuele servers
    - +/- 6.000 werkplekken
    - Rest BYOD

Indicatie omvang omgeving MBO-instelling

Onderstaande indicatie is gebaseerd op cijfers van enkele gemiddelde MBO-instelling.

Gemiddelde MBO-instelling:

Aantal users:

- +/- 12.000 studenten
- +/- 1.500 medewerkers (1200 FTE)

Indicatie verkeer:

- +/- 2.000 Mbps piek netwerkverkeer door netwerksensoren
- +/- 3.500 concurrent ip-systemen op het netwerk (zowel gast als managed), waarvan:
    - +/- 110 servers (20 fysiek, de rest virtueel)
    - +/- 400 werkplekken volledig in beheer
    - +/- 800 werkplekken gedeeltelijk in beheer (security policies)
    - Rest BYOD

Toelichting begrippen

Ter verduidelijking worden hieronder enkele begrippen toegelicht van hetgeen binnen deze scope afgedekt wordt en dus – naast de andere onderdelen die in de scope zijn opgenomen – door Opdrachtnemer geleverd dienen te worden:

- Security Monitoring: is het geautomatiseerde proces van het verzamelen en analyseren (inclusief filtering, correlatie en prioritering) van indicatoren van potentiële beveiligingsbedreigingen, en vervolgens het uitvoeren van de triage hierop om te komen tot passende acties. Om het verzamelen en analyseren van informatie over verdacht gedrag of ongeautoriseerde systeemwijzigingen in het netwerk te detecteren, is vooraf bepaald en in tooling geïmplementeerd welke soorten gedrag waarschuwingen moeten activeren inclusief passende acties hierop. De benodigde tooling dient door Opdrachtnemer verzorgd te worden;
- Security Incident Management: het proces van het realtime identificeren, beheren, vastleggen en analyseren van beveiligingsdreigingen of -incidenten. Het beoogt een robuust en uitgebreid beeld te geven van beveiligingsproblemen binnen het netwerk. In de gewenste situatie is het de bedoeling dat Opdrachtnemer de gevonden incidenten rapporteert aan SURF en de betreffende Instelling, zodat de Instelling hier vervolgens de passende maatregelen op kan nemen;
- Threat Intelligence: omvat het continue verzamelen van en periodiek rapporteren en adviseren over (niet) technische informatie ten aanzien van dreigingen, kwetsbaarheden en risico's relevant voor het netwerk, dienstverlening en sector waarbinnen de Instellingen opereren. Op basis van diverse bronnen, zowel commercieel als publiekelijk beschikbaar, met informatie over actuele dreigingen dient Opdrachtnemer automatisch informatie te aggregeren en correleren met aangesloten logbestanden/systemen;
- Security Analysis: is het specifieke proces van het realtime analyseren en beoordelen van beveiligingsdreigingen of -incidenten. Over het algemeen maakt Security Analysis integraal onderdeel uit van Security Incident Management. In de gewenste situatie is het de bedoeling dat Opdrachtnemer over de uitgevoerde analyses rapporteert aan SURF en Instellingen, zodat hier vervolgens de passende maatregelen genomen kunnen worden.