

Opdrachtomschrijving Perimeter Firewall SURF

Beschrijving huidige en gewenste situatie

SURF levert vanuit datacenters in Amsterdam diensten waaronder High Performance Compute en High Capacity Storage oplossingen. Daarmee worden aangesloten onderwijs- en onderzoeksinstellingen verspreid over de hele wereld bediend.

Algemene informatie huidige situatie

SURF maakt in Amsterdam gebruik van 3 datacenter locaties (3DC):

- Digital Realty AMS17 - groot, hoofdlocatie, 203 racks
- interxion AM1 - middel, 8 racks
- interxion AM8 - middel, 8 racks

De locaties kennen een eenduidig network securitybeleid en zijn redundant en gelijkwaardig opgebouwd. Zij kunnen in geval van calamiteiten als standalone locatie online blijven. Hiermee wordt de dienstverlening gewaarborgd en kan de impact van eventuele verstoringen tot een minimum worden beperkt. Op alle locaties wordt gebruikt gemaakt van standaard 19" racks en redundante ontsloten voeding.

De netwerk infrastructuur bestaat uit High-End routers (datacenter core), open networking switches (datacenter EVPN) en FortiGate firewalls (security). Er wordt gebruik gemaakt van meerdere redundante 100Gbps WAN verbindingen tussen de datacenter locaties en de aangesloten interne- en externe netwerken.

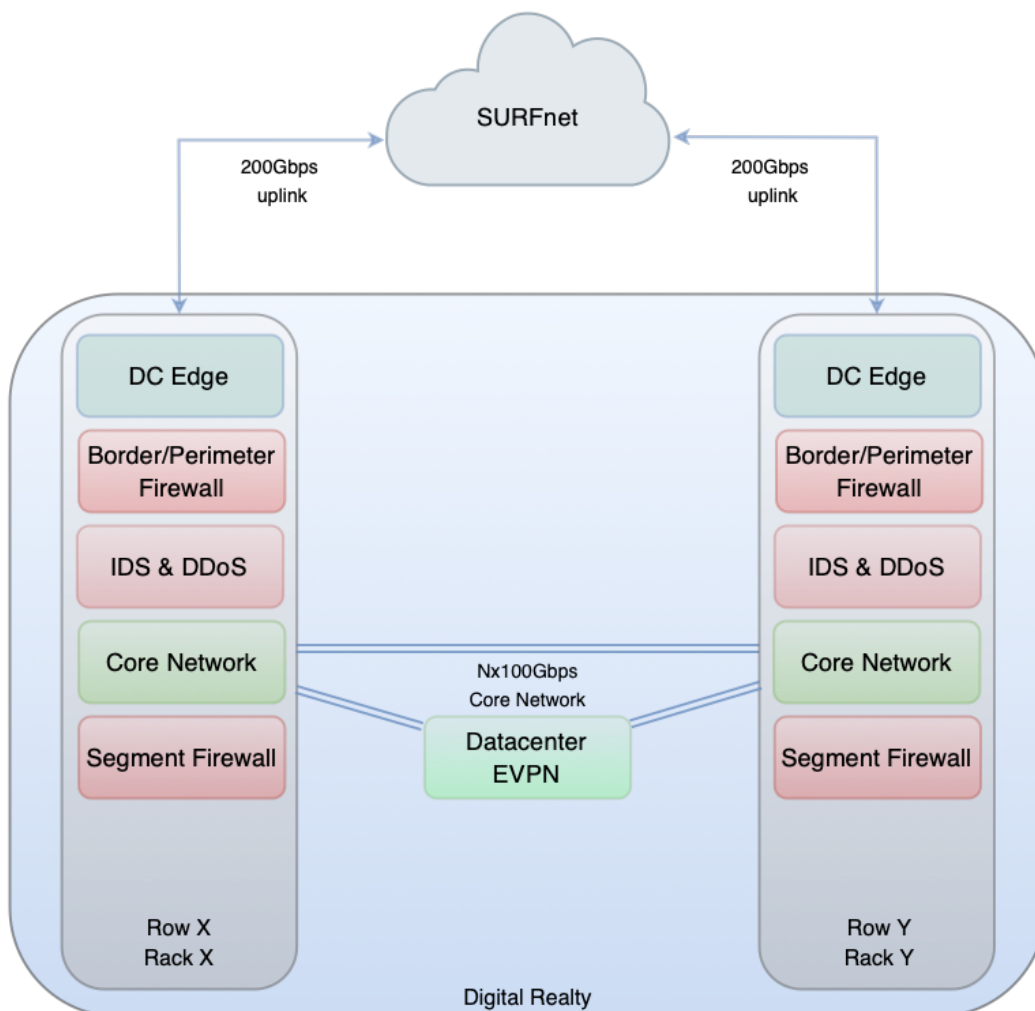
Naar verwachting zullen de uplinks naar het Internet in de komende 3-5 jaar groeien naar 2x 400Gbps en verder. Deze grote hoeveelheden extern verkeer zullen door een nieuw te plaatsen Perimeter Firewall worden gefilterd en afgehandeld.

Technische informatie huidige situatie

- Redundante 2x 100Gbps uplinks naar internet, groei naar 2x 200Gbps.
- Meerdere externe 100Gbps WAN verbindingen (OPN, T1) out of scope voor firewall
- Intern DC verkeer (East-West) wordt door een gelaagd security model gefilterd en afgehandeld. Filtering gebeurt ofwel host-based, ofwel door de Segment Firewall.
- Extern DC verkeer (North-South) wordt door ofwel door netwerkkapparatuur (ACLs) ofwel door de huidige Segment Firewall gefilterd.
- Er is geen stateful firewall actief op de uplinks voor extern verkeer.
- Er zijn beperkte mogelijkheden voor het filteren van extern ipv6 verkeer.
- IDS/IPS zal door een dedicated oplossing icm een Packet Broker uitgevoerd gaan worden. Dit valt buiten de scope van de nieuwe Perimeter Firewall.

Beschrijving gewenste situatie

Het uitgangspunt van dit target design is een schaalbare en redundante network security infrastructuur. De gewenste situatie wordt in onderstaande tekening weergegeven:



Dit specifieke design beschrijft de gewenste situatie op de hoofdlocatie Digital Realty.

De Perimeter Firewall is als een High Availability cluster geïmplementeerd om redundantie en beschikbaarheid te garanderen. In het geval van een verstoring of calamiteit vindt een failover plaats naar de standby unit. Daarbij worden policies en actieve firewall sessies behouden waardoor de impact op het productie verkeer zoveel als mogelijk beperkt wordt.

Binnen het datacenter zijn de 2 firewall units fysiek van elkaar gescheiden. De units zijn beide in een aparte rij geplaatst, om de impact van het uitvallen van voeding- of netwerkverbindingen te minimaliseren. Daarmee wordt het design van het Core Network gevolgd, waar dezelfde fysieke scheiding is aangebracht.

De Perimeter Firewall heeft als belangrijkste taak het toepassen van stateful filtering en network access control op het externe datacenter verkeer (North-South). DDoS protection zal door de Perimeter Firewall uitgevoerd gaan worden in een combinatie met de NaWas anti-DDoS services. Overige security services zoals IDS/IPS worden door een dedicated oplossing binnen het datacenter geleverd.

Intern datacenter verkeer (East-West) wordt door de Segment Firewall en/of host-based firewalls gefilterd en afgehandeld. Het gaat hier om verkeer tussen de verschillende diensten en aangesloten netwerken. De Segment Firewall is, net als de Perimeter Firewall, als High Availability cluster geïmplementeerd.

De DC Edge en het Core Network garanderen schaalbaarheid, redundantie en beschikbaarheid. De Perimeter Firewall is redundant aan deze netwerk zones gekoppeld waardoor impact bij verstoringen tot het minimale wordt beperkt.

Technische informatie target design

Om de huidige- en toekomstige groei van het netwerk te faciliteren, moet de Perimeter Firewall moet ten minste over de volgende specificaties beschikken:

- 8x 100GE QSFP poorten en 16x 25GE SFP28 poorten.
- Minimale doorvoersnelheid van ten minste 800 Gbps voor firewall traffic
- Ondersteuning voor meerdere gelijktijdige 100Gbps Elephant flows*
- High Availability cluster in een active/passive of active/active opstelling.
- Upstream/downstream switches maken gebruik van MLAG of vergelijkbaar multi-chassis protocol om op de active/passive firewall te worden ontsloten.
- Stateful traffic filtering, geo-blocking, en black-/whitelisting policies voor ipv4 en ipv6 verkeer.
- Minimaal 100.000 unieke firewall policies
- Mogelijkheid voor een dedicated management oplossing voor alle firewalls, waarbij de management- en analyse functionaliteiten separaat van elkaar geïmplementeerd kunnen worden (ivm redundantie).
- Mogelijkheid om gebruik te maken van threat intelligence icm DDoS- en IDS functionaliteiten.

* Elephant flows zijn extreem grote datasets welke binnen een enkele TCP sessie worden afgehandeld. Onvoldoende capaciteit om dit type verkeer af te handelen kan een grote impact hebben op het overige netwerkverkeer dat door een firewall wordt afgehandeld.

Implementatie

De Perimeter Firewall zal uiterlijk in Q4 2022 op de hoofdlocatie Digital Realty geïmplementeerd worden. Het target design zal optioneel in een later stadium en op een kleinere schaal ook in de overige 2 datacenters worden geïmplementeerd. Het doel hiervan is een identieke netwerk security infrastructuur met zoveel mogelijk identieke security policies en services op alle locaties.

Voor de implementatie op Digital Realty is onderstaande globale planning opgesteld:

Sub-taak	Beschrijving	Planning
Aanbestedingstraject	Startdatum overeenkomst	1 aug 2022
Proof of Concept	Proof of Concept binnen de acceptatie fase	*
Datum levering	Uiterlijke datum levering hardware	Week 48
Implementatie Firewall	Implementatie firewall cluster op Digital Realty	Week 49
Migratie en test	Migratie + testen productieverkeer	Week 50
Optimalisatie fase	Optimalisatie van policies en configuratie	-
Productie	De firewall is in bedrijf	Week 1

* Afhankelijk van specificaties Proof of Concept, planning en beschikbaarheid.