

# Firewall as a Service

- Benodigdheden nieuwe aanvraag
- Minor change aanvragen
- Rapportage aanvragen

# Benodigdheden nieuwe aanvraag

## Inleiding

Voor het maken van een nieuwe wijzigingsaanvraag zijn enkele gegevens essentieel, dit document geeft inzicht in welke gegevens er aangeleverd dienen te worden.

## Aanvraag

### Firewall regels/ACL's

Bij het indienen van een firewall regel aanvraag dient u de volgende gegevens aan te leveren:

- Doel van de aanvraag. Ofwel voor welke toepassing is het, een korte omschrijving van de applicatie.
- De richting van het verkeer; Naar binnen, naar buiten, tussen interne netwerken.
- Bron IP adres/reeks/netwerk. Waar komt het verkeer vandaan.
- Doel IP adres/reeks/netwerk. Waar gaat het verkeer naartoe.
- Welke poorten. Welke TCP of UDP poorten dienen opengezet te worden.

## Interface

Indien er een additionele interface moet worden geconfigureerd dient u de volgende gegevens aan te leveren:

- IP adres. Welk IP adres moet de interface krijgen.
- Subnet masker. Welk subnet masker krijgt de interface.
- VLAN ID. Indien het een VLAN interface betreft, welk VLAN ID.
- Fysieke interface nr. Welke fysieke poort wilt u aansluiten? Kan ook VLAN interface zijn.
- Eventuele routes. Zijn er routes die er over deze interface gerouteerd moeten worden.



# Minor change aanvragen

De volgende gegevens zijn verplicht voor het aanvragen van een configuratiewijziging. Zonder deze gegevens kunnen wij de aanvraag niet verwerken.

Onderaan de pagina vindt u een word document die u kunt invullen en opsturen naar [servicedesk-ms@centralpoint.nl](mailto:servicedesk-ms@centralpoint.nl). De Servicedesk beoordeelt het formulier en laat u weten wanneer de wijziging wordt uitgevoerd.

## Algemene informatie

Vul onderstaand formulier aan met algemene informatie. Onder dit formulier vindt u specifieke formulieren voor wijzigingen in interface(s), routing, policies, vips of UTM.

| Vraag                                       | Antwoord | Opmerking   |
|---|----------|---|
| Welk type prioriteit heeft de wijziging     |          | Maak een keuze uit <b>niet urgent</b> of <b>urgent</b>  |
| Welk onderdeel dient er gewijzigd te worden |          | Maak een keuze uit <b>interface, routing, policy, vip, UTM</b> of <b>overige</b> . <i>Indien uw keuze hier niet tussenstaat, dan betreft het een major change. Neem hiervoor contact op met de Servicedesk.</i> |
| Wat verwacht u van de wijziging             |          | Wat is uw wens? In geval van een policy change kan dit zijn: het openstellen van een publieke dienst of het blokkeren van een computer  |
| Opmerking(en)                               |          | Heeft u nog overige informatie?   |

## Interface

Vul de volgende tabel zo volledig mogelijk aan

| Vraag   | Antwoord |
|---|----------|
| Welke interface dient er aangepast te worden                    |          |
| Welk ip adres moet de interface krijgen (kan ook een VLAN zijn) |          |

| Vraag   | Antwoord |
|---|----------|
| Welke services moeten er geactiveerd worden (administrative access, DHCP of device detection) |          |

## Routing

Vul de volgende tabel zo volledig mogelijk aan

| Vraag                                      | Antwoord |
|--|----------|
| Om welk type routing gaat het              |          |
| Welke gegevens moeten er toegevoegd worden |          |

## Policy

Vul de volgende tabel zo volledig mogelijk aan

| Vraag  | Antwoord |
|--|----------|
| Welke naam moet de policy krijgen                              |          |
| Welke interface is incoming                                    |          |
| Welke interface is outgoing                                    |          |
| Wat is de source   |          |
| Wat is de destination  |          |
| Welke schedule wenst u   |          |
| Welke services moeten er toegestaan worden                     |          |
| Moet het verkeer worden toegestaan of juist worden geblokkeerd |          |
| Moet NAT worden aangezet                                       |          |
| Moet IP Pool geactiveerd worden                                |          |
| Moeten er security profiles geactiveerd worden                 |          |
| Moet het verkeer gelogd worden                                 |          |

## Virtual IP

Vul de volgende tabel zo volledig mogelijk aan

| Vraag   | Antwoord |
|---|----------|
| Welke naam moet het Virtual IP krijgen                              |          |
| Op welk publiek ip adres moet de service beschikbaar worden gesteld |          |
| Op welke destination ip moet het verkeer gestuurd worden            |          |
| Welk protocol wordt er gebruikt (udp of tcp)                        |          |
| Wat is de source port   |          |
| Wat is de destination port  |          |

## UTM

Vul de volgende tabel zo volledig mogelijk aan

## Whitelisting

Wordt er een website geblokkeerd die legitiem is? Of moet er juist een website geblokkeerd worden?

| Vraag                                     | Antwoord |
|---|----------|
| Om welke website gaat het                 |          |
| Wat moet er gebeuren (blokkeren/toelaten) |          |
| Exacte URL                                |          |

# Rapportage aanvragen

## Mogelijkheden

De Fortimanager verzamelt veilig de log-data van Fortinet devices en andere syslog-compatible devices. Een uitgebreid scala van eenvoudig op maat te maken rapporten stellen u in staat om te analyseren, rapporteren en archiveren van beveiligingsvoorvallen, data verkeer, web content en e-mail-data om zo te voldoen aan uw compliance beleid.

## Aanvraagformulier

Dit formulier dient zo volledig mogelijk ingevuld te worden. Indien er velden niet ingevuld worden is het voor ons niet mogelijk om de rapportage aan te maken.

| Veld                       | Waarde |
|----------------------------|--------|
| Aanvrager                  |        |
| Periode                    |        |
| Herhaling                  |        |
| Notificatie e-mail adres * |        |

\* De rapportages worden naar het opgegeven e-mailadres verstuurd.

De volgende rapporten zijn door Infotheek ICT Services voor u samengesteld:

| Item                              | Bevat onderdelen  |
|-----------------------------------|---|
| Admin and System Events Report    | Login overzicht - List of Failed Logins - System Events - Events by category (critical, high, medium etc.)  |
| Bandwidth and Applications Report | Bandbreedte overzicht - Sessie overzicht - Verkeer statistieken - Top 30 applicatie bandbreedte verbruik - Top 30 gebruikers bandbreedte gebruik - Top 30 destination bandbreedte gebruik |

| Item              | Bevat onderdelen   |
|-------------------|--|
| Security Analysis | Top users bandbreedte - Top users sessies - Top destination bandbreedte - Top destination sessies - DHCP summary - Malware detected - Malware victims - Malware source - Botnet detected - Intrusion detected - Intrusion victims - Foutieve inlog pogingen - Kritische systeem events |
| Threat Report     | Malware detected - malware victims - malware source - malware timeline - botnet detected - botnet victims - botnet C&C - botnet timeline - intrusions detected - intrusion victims - intrusion sources - intrusion blocked - intrusion timeline  |