



Hos Linux-Hus.dk tilbyder vi både en hosted firewall og en decentral løsning.

Hvad enten du vælger en hosted firewall, som placeres centralt i vores datacenter, eller en decentral løsning, som leveres på din virksomheds adresse, så er begge løsninger overvåget og sikret døgnet rundt af Linux-Hus Network Operation Center.

Vi tilbyder tre forskellige firewall-løsninger afhængig af din virksomheds behov:

- Lille firewall
- Mellem firewall
- Stor firewall

Hos Linux-Hus tilbyder vi samtidig, at konfigurere din firewall-løsning ud fra tre forskellige setups:

- Restriktivt setup (Tillader meget lidt trafik)
- Løst setup (Tillader det meste trafik)
- Tomt setup (Al trafik tilladt)

Her kan du læse mere indgående om de tre løsninger der passer til din virksomheds behov.

1. Introduktion og 2. Teknik

1. Introduktion til Hosted Firewall

Linux-Hus tilbyder med sin firewall en af markedets bedste sikkerhedsløsninger i et enkelt og simpelt setup, som sikrer din virksomheds netværkstrafik og data. Løsningen er dedikeret og baseret på produkter fra ClearOS/Pfsense og implementeret direkte i vores backbone - med mulighed for at indbygge redundans for maksimal opetid.

Linux-Hus tilbyder 2 typer af løsninger for Hosted Firewalls

- Managed hvor det er Linux-Hus der står for konfiguration, overvågning samt backup af konfiguration
- Selfmanaged hvor kunden selv står for konfiguration samt overvågning, Linux-Hus leverer et initialt set-up se afsnit 6

2. Teknisk opbygning

Linux-Hus Hostede Firewall løsning bliver leveret centralt i Linux-Hus datacenter og der kan opbygges et fuldt redundant setup Nedenstående principskitse viser løsningen som tilbydes, der er ikke forskel på det tekniske setup på de 2 typer af løsninger (managed og selfmanaged). Løsning everes på trunk op i mod vores MPLS VPN net og kunden har mulighed for både internet og MPLS VPN.

Der kan opbygges et fuldt redundant setup som vist nedenfor. Der etableres redundans via delt gateway-adresse. Løsningen vil kræve etablering af HA (high availability) i mellem de 2 Firewalls. Redundans laves som et active/standby setup.

3. Firewall modeller

Linux-Hus tilbyder tre forskellige firewall modeller afhængig af kundens behov. Følgende er gældende for alle tre modeller:

- Statisk routing
- NAT
- Stateful inspection på følgende protokoller: CTIQBE, DCE/RPC, DNS, ESMTP, FTP, GTP, H.323, HTTP, ICMP, ILS, MGCP, NetBIOS, PPTP, RSH, RTSP, SIP, Skinny, SMTP, SNMP, SQLNET, SunRPC, TFTP, WAAS, XDMCP
- DNS Doctoring pr. host ved 1:1 NAT, samt DNS Doctoring for en enkelt host ved PAT (n:1 NAT)
- Overvågning afhænger af den valgte løsning med mulighed for 24/7 overvågning

3.1. Lille Firewall

Lille firewall understøtter følgende specifikationer:

- 15.000 nye forbindelser pr. sekund
- 250.000 samtidige forbindelser
- Garanteret 250 Mbps throughput
- Op til 350 Mbps throughput afhængig af pakkestørrelse

3.2. Mellem Firewall

Mellem firewall understøtter følgende specifikationer:

- 20.000 nye forbindelser pr. sekund
- 500.000 samtidige forbindelser
- Garanteret 350 Mbps throughput
- Op til 650 Mbps throughput afhængig af pakkestørrelse

3.3. Stor Firewall

Stor firewall understøtter følgende specifikationer:

- 30.000 nye forbindelser pr. sekund
- 750.000 samtidige forbindelser
- Garanteret 450 Mbps throughput
- Op til 1000 Mbps throughput afhængig af pakkestørrelse

4. Konfigurationer for Managed Firewall

4. Konfigurationer for Managed Firewall

Linux-Hus tilbyder ved levering af en Managed Firewall 3 forskellige konfigurationer, et restriktivt setup, et løst setup eller et custom setup. Disse konfigurationer er beskrevet i nedenstående afsnit.

4.1. Restriktivt setup

Som udgangspunkt er al trafik blokeret, men følgende porte er åbnet for trafik initialiseret fra indersiden mod internettet:

- Web-browsere (Port 80 TCP og 443 TCP / http: og https:)
- SSH (Port 22 TCP)
- DNS (Port 53 UDP og TCP)
- NTP (Port 123 UDP og TCP)

4.2. Løst setup

Alle TCP-sessioner, som er initialiseret fra indersiden mod internettet, er tilladte, samt følgende UDP-porte:

- DNS (port 53)
- NTP (port 123)

4.3. Custom setup

Ønsket kunde en kundetilpasset konfiguration afregnes efter antallet af regler kunden ønsker at få oprettet. Der er mulighed for at vælge produktpakke til hhv. 0-10 regler og 0- 20 regler.

5. Tillægsydelser til Managed Firewall

5. Tillægsydelser til Managed Firewall

Følgende tillægsydelser kan købes sammen med firewall løsningen eller bestilles efterfølgende:

- Ekstra VRF/DMZ i firewall
- SNMP read
- SSL VPN (på Linux-Hus VPN koncentrator)

5.1. Ændringer i konfiguration

Følgende ændringer er indeholdt i prisen for Managed Firewall, Linux-Hus bestræber sig på, at ændringsanmodninger vil blive behandlet inden for 5 arbejdsdage efter Kunden og Linux-Hus er blevet enige om ændringsanmodningens art.:

- Ændringer/tilføjelser i NAT regler
- Ændringer/tilføjelser i Firewall regler

Alle andre ændringer er ikke indeholdt i prisen og vil blive opkrævet særskilt.

6. - 11.

6. Konfiguration for Selfmanaged Firewall

Linux-Hus leverer firewall'en med et initial set-up som sikre at firewall'en kan tilgås samtidig oprettes der bruger login for kunden og for Linux-Hus. Kunden overtager herefter ansvaret for konfiguration og overvågning af firewall. Bemærk at hvis kunde sletter Linux-Hus bruger og adgang, er det ikke længere muligt at tilkøbe hjælp fra Linux-Hus.

7. Tillægsydelser til Selfmanaged Firewall

Ønskes hjælp af Linux-Hus tilkøbes dette på konsulentbasis. Nyere software leveres ved forespørgsel til Linux-Hus. Derud over kan følgende tillægsydelser købes sammen med firewall løsningen eller bestilles efterfølgende. - Ekstra VRF - Licensnøgle til brugere af SSL VPN (samtidige) - Klippekort til support

8. Forudsætninger

Kunden skal bruge Linux-Hus som internetleverandør. Firewall placeret i Linux-Hus datacenter forudsætter ét af følgende produkter fra Linux-Hus: - Fiberforbindelse - Private Cloud - Virtuel Server - Co-location

9. Begrænsninger

Managed Firewall, løsningen understøtter ikke dynamiske routningsprotokoller og IPv6. Self-managed ifølge Specifikationer.

10. Servicetilgængelighed

For Hosted Firewall differentieres der mellem enkelte forbindelser og redundante forbindelser. I nedenstående skema redegøres der for den garanterede opetid.

Hosted Firewall	Enkelt forbindelse	Redundant forbindelse ¹
Garanteret opetid	99.7 %	99.9 %

Firewall er underlagt Service Level Agreement for datacenterforbindelsen.

11. Betingelser

Leveringstiden er op til 4 uger, med mindre andet står skrevet i kontrakten. Leveringstiden forudsætter en eksisterende forbindelse. Bestilles firewall løsningen sammen med en forbindelse, så gælder samme leveringstid, som ved forbindelsen. Linux-Hus er ikke ansvarlig for sikkerhedsbrud hos kunden. Linux-Hus assisterer ikke med vejledning i sikkerhedspolitikker. Linux-Hus kan ikke gøres ansvarlig for DDOS angreb eller andre typer angreb imod Kundens firewall.