Fortinet FortiGate As Built Report

|  |  |
| --- | --- |
| Author: | As Build Report for Fortigate |
| Date: | dimanche 31 juillet 2022 |
| Version: | 1.0 |

# 1 Implementation Report FGT2KE3917900165

The following section provides a summary of the implemented components on the Fortinet FortiGate infrastructure.

## 1.1 FortiCare

The following section details FortiCare settings configured on FortiGate.

|  |  |
| --- | --- |
| Model | FGT2KE |
| Serial | FGT2KE3917900165 |
| Status | registered |
| Account | tmgfortinet@gmail.com |
| Company | TMG@Fortinet |

Table - FortiCare

The following section details support settings configured on FortiGate.

| Type | Level | Status | Expiration Date |
| --- | --- | --- | --- |
| Hardware | Advanced HW | licensed | 02/01/2026 |
| Enhanced | Premium | licensed | 02/01/2026 |

Table - Support

The following section details firmware information on FortiGate.

|  |  |
| --- | --- |
| Installed | v7.2.0 |
| Update | No Update Available |
| Upgrade Path | N/A |

Table - Firmware

## 1.2 System

The following section details system settings configured on FortiGate.

### 1.2.1 Global

|  |  |
| --- | --- |
| Nom | NGFW\_PRI |
| Alias | FG1K5D3I16800732 |
| Reboot | Everyday at 00:00 |
| Port SSH | 22 |
| Port HTTP | 80 |
| Port HTTPS | 443 |
| HTTPS Redirect | enable |

Table - Global

### 1.2.2 Settings

|  |  |
| --- | --- |
| OP Mode | nat |
| Central NAT | disable |
| LLDP Reception | global |
| LLDP Transmission | global |
| Comments |  |

Table - Settings

### 1.2.3 GUI Settings

|  |  |
| --- | --- |
| Language | english |
| Theme | jade |
| IPv6 | enable |
| Wireless Open Security | enable |
| Implicit Policy | enable |
| Dns Database | enable |
| Load Balance | disable |
| Explicit Proxy | enable |
| Dynamic Routing | enable |
| Application Control | enable |
| IPS | enable |
| VPN | enable |
| Wireless Controller | enable |
| Switch Controller | enable |
| WAN Load Balancing (SDWAN) | enable |
| Antivirus | enable |
| Web Filter | enable |
| Video Filter | enable |
| DNS Filter | enable |
| WAF Profile | enable |
| Allow Unnamed Policy | enable |
| Multiple Interface Policy | enable |
| ZTNA | enable |
| OT | enable |

Table - Settings

### 1.2.4 DNS

|  |  |
| --- | --- |
| Primary | 96.45.45.45 |
| Secondary | 96.45.46.46 |
| Domain | fortidemo.com |
| Protocol | dot |

Table - DNS

### 1.2.5 DNS Server

| Name | Mode | DNS Filter Profile | DOH |
| --- | --- | --- | --- |
| FortiLink | forward-only | default | disable |

Table - DNS Server

### 1.2.6 Admin

| Name | Profile | Trusted Hosts | MFA |
| --- | --- | --- | --- |
| demo | ReadOnly | 0.0.0.0 0.0.0.00.0.0.0 0.0.0.00.0.0.0 0.0.0.00.0.0.0 0.0.0.00.0.0.0 0.0.0.00.0.0.0 0.0.0.00.0.0.0 0.0.0.00.0.0.0 0.0.0.00.0.0.0 0.0.0.00.0.0.0 0.0.0.0 | disable |

Table - Administrator

### 1.2.7 Interfaces

| Name | Alias | Role | Description | Type | Vlan ID | Mode | IP Address | Allow Access | DHCP Relais | Status | Speed |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| DCFW | DCFW | lan |  | vlan | 2 | static | 10.88.2.254/255.255.255.0 | ping https ssh snmp fgfm fabric ftm | "10.88.210.102" "10.88.210.50" | up | auto |
| FITNUC |  | lan |  | vlan | 111 | static | 10.100.1.254/255.255.255.0 | ssh fabric |  | up | auto |
| FSA-DMZ |  | lan |  | vlan | 23 | static | 10.88.23.1/255.255.255.0 | ping https ssh fgfm fabric |  | up | auto |
| FSA-DMZ2 |  | lan |  | vlan | 41 | static | 10.88.41.254/255.255.255.0 | ping https ssh |  | up | auto |
| FWLC | MeruWLC | lan |  | vlan | 51 | static | 10.88.51.254/255.255.255.0 | ping https ssh fgfm fabric | "10.88.210.102" "10.88.210.50" | up | auto |
| FortiLink | FSW-AGG | undefined |  | aggregate | 0 | static | 169.254.1.1/255.255.255.0 | ping fabric |  | up | auto |
| ISFW-HA |  | lan |  | vlan | 12 | static | 10.88.12.254/255.255.255.0 | ping https ssh snmp http fgfm radius-acct fabric ftm | "10.88.210.102" "10.88.210.50" | up | auto |
| P22 |  | lan |  | vlan | 11 | static | 10.88.11.99/255.255.255.0 | ping https ssh |  | up | auto |
| UNUSED |  | lan |  | switch | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| VPN-MPLS1 |  | undefined |  | tunnel | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| WLC-Staff | WLC-Staff | lan |  | vlan | 54 | static | 10.88.54.254/255.255.255.0 | ping https ssh snmp fgfm fabric | "10.88.210.102" "10.88.210.50" | up | auto |
| WLC-Students | WLC-Students | lan |  | vlan | 53 | static | 10.88.53.254/255.255.255.0 | ping https ssh snmp fgfm | "10.88.210.102" "10.88.210.50" | up | auto |
| WLC-Teachers | WLC-Teachers | lan |  | vlan | 52 | static | 10.88.52.254/255.255.255.0 | ping https ssh snmp fgfm | "10.88.210.106" "10.88.210.50" | up | auto |
| cam.FortiLink |  | undefined | Forticamera VLAN | vlan | 4090 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| l2t.root |  | undefined |  | tunnel | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| mgmt1 |  | lan |  | physical | 0 | static | 192.168.1.99/255.255.255.0 | ping https ssh fgfm |  | up | auto |
| mgmt2 |  | lan |  | physical | 0 | static | 172.30.73.33/255.255.255.0 | ping https fgfm |  | up | auto |
| modem |  | undefined |  | physical | 0 | pppoe | 0.0.0.0/0.0.0.0 |  |  | down | auto |
| nac\_segment | nac\_segment.FortiLink | undefined | NAC Segment VLAN | vlan | 4088 | static | 10.255.11.1/255.255.255.0 |  |  | up | auto |
| naf.root |  | undefined |  | tunnel | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| onboarding |  | undefined | NAC Onboarding VLAN | vlan | 4089 | static | 169.254.11.1/255.255.255.0 |  |  | up | auto |
| port1 | HA | lan |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port2 | HA | lan |  | physical | 0 | static | 0.0.0.0/0.0.0.0 | fabric |  | up | auto |
| port3 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port4 |  | lan |  | physical | 0 | static | 192.168.20.1/255.255.255.0 | ping https http fabric |  | up | auto |
| port5 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port6 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port7 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port8 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port9 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port10 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port11 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port12 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port13 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port14 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port15 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port16 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port17 |  | lan | ToWAN | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port18 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port19 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port20 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port21 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port22 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port23 | WAN1-MPLS | wan |  | physical | 0 | static | 10.168.167.10/255.255.255.0 | ping ssh fgfm |  | up | auto |
| port24 | WAN2-Broadband | wan |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port25 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port26 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port27 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port28 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port29 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port30 |  | lan |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port31 |  | lan | ISFW | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port32 |  | lan |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port33 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port34 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port35 |  | undefined |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port36 | WAN\_Uplink | wan |  | physical | 0 | static | 172.30.72.33/255.255.255.0 | ping https ssh snmp fgfm fabric |  | up | auto |
| port37 | HA-Link1 | lan |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| port38 | HA-Link2 | lan |  | physical | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| qtn.FortiLink |  | undefined | Quarantine VLAN | vlan | 4093 | static | 10.254.254.254/255.255.255.0 |  |  | up | auto |
| snf.FortiLink |  | undefined | Sniffer VLAN | vlan | 4092 | static | 10.254.253.254/255.255.254.0 | ping |  | up | auto |
| ssl.root | SSL VPN interface | undefined |  | tunnel | 0 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| test |  | lan |  | vlan | 100 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| voi.FortiLink |  | undefined | Fortivoice VLAN | vlan | 4091 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |
| vsw.FortiLink |  | undefined |  | vlan | 1 | static | 0.0.0.0/0.0.0.0 |  |  | up | auto |

Table - Interface

## 1.3 Route

The following section details route settings configured on FortiGate.

### 1.3.1 Summary

The following section prrovides a summary of route settings.

|  |  |
| --- | --- |
| Monitor Route | 26 |
| Static Route | 10 |
| Policy Based Route | 0 |

Table - Summary

### 1.3.2 Route Monitor

| Type | IP/Mask | Gateway | Interface | Distance/Metric/Priority |
| --- | --- | --- | --- | --- |
| static | 0.0.0.0/0 | 172.30.72.254 | port36 | 10 / 0 / 1 |
| connect | 10.88.2.0/24 | 0.0.0.0 | DCFW | 0 / 0 / 0 |
| connect | 10.88.11.0/24 | 0.0.0.0 | P22 | 0 / 0 / 0 |
| connect | 10.88.12.0/24 | 0.0.0.0 | ISFW-HA | 0 / 0 / 0 |
| connect | 10.88.23.0/24 | 0.0.0.0 | FSA-DMZ | 0 / 0 / 0 |
| connect | 10.88.41.0/24 | 0.0.0.0 | FSA-DMZ2 | 0 / 0 / 0 |
| connect | 10.88.51.0/24 | 0.0.0.0 | FWLC | 0 / 0 / 0 |
| connect | 10.88.52.0/24 | 0.0.0.0 | WLC-Teachers | 0 / 0 / 0 |
| connect | 10.88.53.0/24 | 0.0.0.0 | WLC-Students | 0 / 0 / 0 |
| connect | 10.88.54.0/24 | 0.0.0.0 | WLC-Staff | 0 / 0 / 0 |
| static | 10.88.101.0/24 | 10.88.12.99 | ISFW-HA | 10 / 0 / 1 |
| static | 10.88.102.0/24 | 10.88.12.99 | ISFW-HA | 10 / 0 / 1 |
| static | 10.88.103.0/24 | 10.88.12.99 | ISFW-HA | 10 / 0 / 1 |
| static | 10.88.110.0/24 | 10.88.12.99 | ISFW-HA | 10 / 0 / 1 |
| static | 10.88.120.0/24 | 10.88.12.99 | ISFW-HA | 10 / 0 / 1 |
| static | 10.88.130.0/24 | 10.88.12.99 | ISFW-HA | 10 / 0 / 1 |
| static | 10.88.210.0/24 | 10.88.2.21 | DCFW | 10 / 0 / 1 |
| static | 10.89.0.0/16 | 10.88.12.99 | ISFW-HA | 10 / 0 / 1 |
| connect | 10.100.1.0/24 | 0.0.0.0 | FITNUC | 0 / 0 / 0 |
| connect | 10.254.252.0/23 | 0.0.0.0 | snf.FortiLink | 0 / 0 / 0 |
| connect | 10.254.254.0/24 | 0.0.0.0 | qtn.FortiLink | 0 / 0 / 0 |
| connect | 10.255.11.0/24 | 0.0.0.0 | nac\_segment | 0 / 0 / 0 |
| connect | 169.254.1.0/24 | 0.0.0.0 | FortiLink | 0 / 0 / 0 |
| connect | 169.254.11.0/24 | 0.0.0.0 | onboarding | 0 / 0 / 0 |
| connect | 172.30.72.0/24 | 0.0.0.0 | port36 | 0 / 0 / 0 |
| connect | 192.168.20.0/24 | 0.0.0.0 | port4 | 0 / 0 / 0 |

Table - Route Monitor

### 1.3.3 Static Route

| Status | Destination | Gateway | Interface | Distance/Weight/Priority |
| --- | --- | --- | --- | --- |
| enable | 0.0.0.0 0.0.0.0 | 172.30.72.254 | port36 | 10 / 0 / 1 |
| enable | 10.88.101.0 255.255.255.0 | 10.88.12.99 | ISFW-HA | 10 / 0 / 1 |
| enable | 10.88.103.0 255.255.255.0 | 10.88.12.99 | ISFW-HA | 10 / 0 / 1 |
| enable | 10.88.110.0 255.255.255.0 | 10.88.12.99 | ISFW-HA | 10 / 0 / 1 |
| enable | 10.88.120.0 255.255.255.0 | 10.88.12.99 | ISFW-HA | 10 / 0 / 1 |
| enable | 10.88.210.0 255.255.255.0 | 10.88.2.21 | DCFW | 10 / 0 / 1 |
| enable | 10.88.130.0 255.255.255.0 | 10.88.12.99 | ISFW-HA | 10 / 0 / 1 |
| enable | 10.88.102.0 255.255.255.0 | 10.88.12.99 | ISFW-HA | 10 / 0 / 1 |
| enable | 10.89.0.0 255.255.0.0 | 10.88.12.99 | ISFW-HA | 10 / 0 / 1 |
| enable | 0.0.0.0 0.0.0.0 | 172.30.73.254 | mgmt2 | 10 / 0 / 1 |

Table - Static Route

## 1.4 Firewall

The following section details firewall settings configured on FortiGate.

### 1.4.1 Summary

The following section prvodies a summary of firewall settings.

|  |  |
| --- | --- |
| Address | 61 |
| Group | 3 |
| IP Pool | 1 |
| Virtual IP | 13 |
| Policy | 17 |

Table - Summary

### 1.4.2 Address

| Name | Type | Value | Interface |
| --- | --- | --- | --- |
| 10.100.10.0 | ipmask | 255.255.255.0/255.255.255.255 |  |
| Cloud\_FAP-Eng | ipmask | 10.88.110.201/255.255.255.255 | FortiLink |
| Cloud\_FAP-Fin | ipmask | 10.88.120.200/255.255.255.255 | FortiLink |
| Cloud\_FAP-Sales | ipmask | 10.88.130.154/255.255.255.255 | FortiLink |
| FABRIC\_DEVICE | ipmask | 0.0.0.0/0.0.0.0 |  |
| FAP-Eng | ipmask | 10.88.110.201/255.255.255.255 | FortiLink |
| FAP-Fin | ipmask | 10.88.120.200/255.255.255.255 | FortiLink |
| FCTEMS0000099518\_Critical | dynamic | 10.88.120.200/255.255.255.255 |  |
| FCTEMS0000099518\_EDR-Classification | dynamic | 10.88.120.200/255.255.255.255 |  |
| FCTEMS0000099518\_Finance | dynamic | 10.88.120.200/255.255.255.255 |  |
| FCTEMS0000099518\_High | dynamic | 10.88.120.200/255.255.255.255 |  |
| FCTEMS0000099518\_Important | dynamic | 10.88.120.200/255.255.255.255 |  |
| FCTEMS0000099518\_Infected | dynamic | 10.88.120.200/255.255.255.255 |  |
| FCTEMS0000099518\_Low | dynamic | 10.88.120.200/255.255.255.255 |  |
| FCTEMS0000099518\_Medium | dynamic | 10.88.120.200/255.255.255.255 |  |
| FCTEMS0000099518\_TEST | dynamic | 10.88.120.200/255.255.255.255 |  |
| FCTEMS0000099518\_Windows 10 | dynamic | 10.88.120.200/255.255.255.255 |  |
| FCTEMS0000099518\_all\_registered\_clients | dynamic | 10.88.120.200/255.255.255.255 |  |
| FCTEMS0000099518\_noav | dynamic | 10.88.120.200/255.255.255.255 |  |
| FCTEMS0000099518\_nos | dynamic | 10.88.120.200/255.255.255.255 |  |
| FCTEMS0000099518\_test | dynamic | 10.88.120.200/255.255.255.255 |  |
| FCTEMS\_ALL\_FORTICLOUD\_SERVERS | dynamic | 10.88.120.200/255.255.255.255 |  |
| FIREWALL\_AUTH\_PORTAL\_ADDRESS | ipmask | 0.0.0.0/0.0.0.0 |  |
| FSA-Admin-sw | ipmask | 10.88.23.8/255.255.255.255 | FSA-DMZ |
| FortiEDR\_31.184.192.80 | iprange | 10.88.23.8/255.255.255.255 |  |
| FortiEDR\_46.161.40.145 | iprange | 10.88.23.8/255.255.255.255 |  |
| FortiEDR\_51.159.95.151 | iprange | 10.88.23.8/255.255.255.255 |  |
| FortiEDR\_67.199.248.10 | iprange | 10.88.23.8/255.255.255.255 |  |
| FortiEDR\_80.38.65.211 | iprange | 10.88.23.8/255.255.255.255 |  |
| FortiEDR\_86.104.134.144 | iprange | 10.88.23.8/255.255.255.255 |  |
| FortiEDR\_87.106.16.115 | iprange | 10.88.23.8/255.255.255.255 |  |
| FortiEDR\_91.231.50.239 | iprange | 10.88.23.8/255.255.255.255 |  |
| FortiEDR\_142.4.205.47 | iprange | 10.88.23.8/255.255.255.255 |  |
| FortiEDR\_142.250.66.174 | iprange | 10.88.23.8/255.255.255.255 |  |
| FortiEDR\_157.122.62.205 | iprange | 10.88.23.8/255.255.255.255 |  |
| FortiEDR\_172.217.14.164 | iprange | 10.88.23.8/255.255.255.255 |  |
| FortiEDR\_173.231.189.26 | iprange | 10.88.23.8/255.255.255.255 |  |
| FortiEDR\_178.33.158.0 | iprange | 10.88.23.8/255.255.255.255 |  |
| FortiEDR\_185.140.53.72 | iprange | 10.88.23.8/255.255.255.255 |  |
| FortiEDR\_185.189.58.222 | iprange | 10.88.23.8/255.255.255.255 |  |
| FortiEDR\_194.165.16.166 | iprange | 10.88.23.8/255.255.255.255 |  |
| FortiEDR\_195.22.26.248 | iprange | 10.88.23.8/255.255.255.255 |  |
| FortiEDR\_203.131.222.102 | iprange | 10.88.23.8/255.255.255.255 |  |
| FortiEDR\_208.105.226.235 | iprange | 10.88.23.8/255.255.255.255 |  |
| MAC\_FCTEMS0000099518\_Critical | dynamic | 10.88.23.8/255.255.255.255 |  |
| MAC\_FCTEMS0000099518\_EDR-Classification | dynamic | 10.88.23.8/255.255.255.255 |  |
| MAC\_FCTEMS0000099518\_Finance | dynamic | 10.88.23.8/255.255.255.255 |  |
| MAC\_FCTEMS0000099518\_High | dynamic | 10.88.23.8/255.255.255.255 |  |
| MAC\_FCTEMS0000099518\_Important | dynamic | 10.88.23.8/255.255.255.255 |  |
| MAC\_FCTEMS0000099518\_Infected | dynamic | 10.88.23.8/255.255.255.255 |  |
| MAC\_FCTEMS0000099518\_Low | dynamic | 10.88.23.8/255.255.255.255 |  |
| MAC\_FCTEMS0000099518\_Medium | dynamic | 10.88.23.8/255.255.255.255 |  |
| MAC\_FCTEMS0000099518\_TEST | dynamic | 10.88.23.8/255.255.255.255 |  |
| MAC\_FCTEMS0000099518\_Windows 10 | dynamic | 10.88.23.8/255.255.255.255 |  |
| MAC\_FCTEMS0000099518\_all\_registered\_clients | dynamic | 10.88.23.8/255.255.255.255 |  |
| MAC\_FCTEMS0000099518\_noav | dynamic | 10.88.23.8/255.255.255.255 |  |
| MAC\_FCTEMS0000099518\_nos | dynamic | 10.88.23.8/255.255.255.255 |  |
| MAC\_FCTEMS0000099518\_test | dynamic | 10.88.23.8/255.255.255.255 |  |
| SSLVPN\_TUNNEL\_ADDR1 | iprange | 10.88.23.8/255.255.255.255 |  |
| VAN\_NAT\_1 | ipmask | 208.91.114.4/255.255.255.255 |  |
| all | ipmask | 0.0.0.0/0.0.0.0 |  |

Table - Address

### 1.4.3 Address Group

| Name | Member | Comment |
| --- | --- | --- |
| BAD\_GUYS | VAN\_NAT\_1 |  |
| FortiEDR\_Malicious\_Destinations | FortiEDR\_91.231.50.239, FortiEDR\_67.199.248.10, FortiEDR\_195.22.26.248, FortiEDR\_173.231.189.26, FortiEDR\_31.184.192.80, FortiEDR\_87.106.16.115, FortiEDR\_178.33.158.0, FortiEDR\_157.122.62.205, FortiEDR\_142.4.205.47, FortiEDR\_185.189.58.222, FortiEDR\_86.104.134.144, FortiEDR\_142.250.66.174, FortiEDR\_208.105.226.235, FortiEDR\_203.131.222.102, FortiEDR\_172.217.14.164, FortiEDR\_46.161.40.145, FortiEDR\_51.159.95.151, FortiEDR\_194.165.16.166, FortiEDR\_80.38.65.211, FortiEDR\_185.140.53.72 | Members of this group will be automatically added by FortiEDR |
| FortiXDR\_Malicious\_Destinations | FortiEDR\_142.4.205.47 |  |

Table - Address Group

### 1.4.4 IP Pool

| Name | Interface | Type | Start IP | End IP | Source Start IP | Source End IP | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| FSAport3 |  | overload | 172.30.72.105 | 172.30.72.105 | 0.0.0.0 | 0.0.0.0 |  |

Table - Virtual IP

### 1.4.5 Virtual IP

| Name | Interface | External IP | Mapped IP | Protocol | External Port | Mapped Port | Comment |
| --- | --- | --- | --- | --- | --- | --- | --- |
| FortiSandbox-VIP | port36 | 172.30.72.80 | 10.88.23.8 | tcp | 0-65535 | 0-65535 |  |
| FortiMail IBE | port36 | 172.30.72.176 | 10.88.11.1 | tcp | 0-65535 | 0-65535 |  |
| FortiGate-DCFW | port36 | 172.30.72.154 | 10.88.2.21 | tcp | 0-65535 | 0-65535 |  |
| FortiSandbox-Slave-IP | port36 | 172.30.72.79 | 10.88.23.9 | tcp | 0-65535 | 0-65535 |  |
| WLC VIP | port36 | 172.30.72.40 | 10.88.51.1 | tcp | 0-65535 | 0-65535 |  |
| FCTEMS\_FWB | port36 | 172.30.72.106 | 10.88.210.101 | tcp | 0-65535 | 0-65535 |  |
| FSIEM\_VIP | port36 | 172.30.72.244 | 10.88.210.32 | tcp | 0-65535 | 0-65535 |  |
| WLM\_VIP | port36 | 172.30.72.41 | 10.88.51.2 | tcp | 0-65535 | 0-65535 |  |
| FortiNAC | port36 | 172.30.72.43 | 10.88.210.50 | tcp | 0-65535 | 0-65535 |  |
| FAC | port36 | 172.30.72.247 | 172.30.72.231 | tcp | 0-65535 | 0-65535 |  |
| FortiManager | port36 | 172.30.72.239 | 10.88.210.253 | tcp | 0-65535 | 0-65535 |  |
| FortiAnalyzer | port36 | 172.30.72.62 | 10.88.210.62 | tcp | 0-65535 | 0-65535 |  |
| LANEdge-VIP | port36 | 172.30.72.156 | 10.88.12.99 | tcp | 0-65535 | 0-65535 |  |

Table - Virtual IP

### 1.4.6 Policy

| Name | From | To | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Block Malicious by FortiEDR | DCFW, FWLC, ISFW-HA, WLC-Staff, WLC-Students, WLC-Teachers | port36 | all | FortiEDR\_Malicious\_Destinations, FortiXDR\_Malicious\_Destinations | ALL | deny | disable | all |  |
| DNS | any | any | all | all | SYSLOG, DNS | accept | enable | all |  |
| FIT - Intel NUC outbound | FITNUC, port4 | port36 | all | all | ALL | accept | enable | all |  |
| Allow FSA Access | FSA-DMZ | port36 | FSA-Admin-sw | all | ALL | accept | enable | utm |  |
| WAN-IBE | port36 | P22 | all | FortiMail IBE | ALL | accept | disable | utm |  |
| IBE-WAN | P22 | port36 | all | all | ALL | accept | disable | utm |  |
| ISFW-WAN | ISFW-HA, DCFW | port36 | all | all | ALL | accept | enable | all | Skip ISFWs will Scan |
| FSA-DMZ-WAN | FSA-DMZ2 | port36 | all | all | ALL | accept | enable | utm |  |
| ISFW-FSA | ISFW-HA, DCFW | FSA-DMZ | all | all | ALL | accept | enable | utm |  |
| Wireless-WLC | WLC-Students, WLC-Staff, WLC-Teachers, FWLC | port36 | all | all | ALL | accept | enable | utm |  |
| IS-DC | ISFW-HA, FWLC, WLC-Staff, WLC-Students, WLC-Teachers | DCFW, ISFW-HA | all | all | ALL | accept | disable | utm |  |
| DC-IS | DCFW, ISFW-HA | ISFW-HA, FWLC, WLC-Staff, WLC-Students, WLC-Teachers | all | all | ALL | accept | disable | all | Reverse of ISFW-DCFW |
| WAN-FWLC-VIP | port36 | FWLC, WLC-Staff, WLC-Students, WLC-Teachers | all | WLC VIP, WLM\_VIP | ALL | accept | disable | all |  |
| FSA-MGMT-VIP | port36 | FSA-DMZ | all | FortiSandbox-VIP, FortiSandbox-Slave-IP | ALL\_ICMP, HTTP, HTTPS, OFTP, SSH, RADIUS | accept | disable | all |  |
| WAN\_DCFW\_VIP | port36 | DCFW | all | FGT\_DCFW\_VIPG | ALL | accept | disable | all |  |
| WAN\_ISFW\_VIP | port36 | ISFW-HA | all | LANEdge-VIP | ALL | accept | disable | all | (Copy of WAN\_DCFW\_VIP) |
| Allow-DNS | any | any | all | all | SYSLOG | accept | enable | all |  |

Table - Policy

## 1.5 User

The following section details user settings configured on FortiGate.

### 1.5.1 Summary

The following section provides a summary of user settings.

|  |  |
| --- | --- |
| User | 0 |
| Group | 2 |
| LDAP | 1 |
| RADIUS | 1 |

Table - Summary

### 1.5.2 User Group

| Name | Type | Member | Match |
| --- | --- | --- | --- |
| RADIUS\_Demo | firewall | FAC-DEMO |  |
| SSO\_Guest\_Users | fsso-service |  |  |

Table - User Group

### 1.5.3 IP Pool

| Name | Server | Port | CN | DN | Type | User |
| --- | --- | --- | --- | --- | --- | --- |
| ad-fortidemo | 10.88.210.100/ | 389 | sAMAccountName | dc=corp,dc=fortidemo,dc=com | regular | administrator@corp.fortidemo.com |

Table - LDAP

### 1.5.4 RADIUS

| Name | Server | Auth Type | NAS-IP |
| --- | --- | --- | --- |
| FAC-DEMO | 172.30.72.232/172.30.72.231 | auto | 0.0.0.0 |

Table - RADIUS