Fortinet FortiGate As Built Report

|  |  |
| --- | --- |
| Author: |  |
| Date: | vendredi 15 mars 2024 |
| Version: | 1.0 |

# 1 Implementation Report FG181FTK22901829

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 | FG181F |
| Serial | FG181FTK22901829 |
| 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 | 17/02/2025 |
| Enhanced | Premium | licensed | 17/02/2025 |

Table - Support

The following section details firmware information on FortiGate.

|  |  |
| --- | --- |
| Installed | v7.4.3 |
| 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 | FortiGate-1801F |
| 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 | security-fabric |
| 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 | All | disable |

Table - Administrator

### 1.2.7 Interfaces

| Name | Alias (Description) | Role | Type | Vlan ID | Mode | IP Address | Status |
| --- | --- | --- | --- | --- | --- | --- | --- |
| DCFW | DCFW | lan | vlan | 2 | static | 10.88.2.254/255.255.255.0 | up |
| FITNUC |  | lan | vlan | 111 | static | 10.100.1.254/255.255.255.0 | up |
| FSA-DMZ |  | lan | vlan | 23 | static | 10.88.23.1/255.255.255.0 | up |
| FSA-DMZ2 |  | lan | vlan | 41 | static | 10.88.41.254/255.255.255.0 | up |
| FWLC | MeruWLC | lan | vlan | 51 | static | 10.88.51.254/255.255.255.0 | up |
| FortiLink | FSW-AGG | n/a | aggregate | 0 | static | 169.254.1.1/255.255.255.0 | up |
| FortiSASE |  | n/a | tunnel | 0 | static | 10.10.1.1/255.255.255.255 | up |
| ISFW-HA |  | lan | vlan | 12 | static | 10.88.12.254/255.255.255.0 | up |
| P22 |  | lan | vlan | 11 | static | 10.88.11.99/255.255.255.0 | up |
| UNUSED |  | lan | switch | 0 | static | 0.0.0.0/0.0.0.0 | up |
| VPN-GCP |  | n/a | tunnel | 0 | static | 0.0.0.0/0.0.0.0 | up |
| VPN-MPLS1 |  | n/a | tunnel | 0 | static | 0.0.0.0/0.0.0.0 | up |
| VPN-SDB |  | n/a | tunnel | 0 | static | 0.0.0.0/0.0.0.0 | up |
| WLC-Staff | WLC-Staff | lan | vlan | 54 | static | 10.88.54.254/255.255.255.0 | up |
| WLC-Students | WLC-Students | lan | vlan | 53 | static | 10.88.53.254/255.255.255.0 | up |
| WLC-Teachers | WLC-Teachers | lan | vlan | 52 | static | 10.88.52.254/255.255.255.0 | up |
| cam.FortiLink | (Forticamera VLAN) | n/a | vlan | 4090 | static | 0.0.0.0/0.0.0.0 | up |
| ha1 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| ha2 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| l2t.root |  | n/a | tunnel | 0 | static | 0.0.0.0/0.0.0.0 | up |
| mgmt1 |  | lan | physical | 0 | static | 192.168.1.99/255.255.255.0 | up |
| mgmt2 |  | wan | physical | 0 | dhcp | 0.0.0.0/0.0.0.0 | up |
| modem |  | n/a | physical | 0 | pppoe | 0.0.0.0/0.0.0.0 | down |
| nac\_segment | nac\_segment.FortiLink(NAC Segment VLAN) | n/a | vlan | 4088 | static | 10.255.11.1/255.255.255.0 | up |
| naf.root |  | n/a | tunnel | 0 | static | 0.0.0.0/0.0.0.0 | up |
| onboarding | (NAC Onboarding VLAN) | n/a | vlan | 4089 | static | 169.254.11.1/255.255.255.0 | up |
| port1 | HA | lan | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port2 | HA | lan | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port3 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port4 |  | lan | physical | 0 | static | 192.168.20.1/255.255.255.0 | up |
| port5 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port6 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port7 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port8 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port9 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port10 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port11 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port12 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port13 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port14 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port15 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port16 | Guest | lan | physical | 0 | static | 10.89.20.10/255.255.255.0 | up |
| port17 | (ToWAN) | lan | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port18 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port19 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port20 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port21 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port22 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port23 | WAN1-MPLS | wan | physical | 0 | static | 10.168.167.10/255.255.255.0 | up |
| port24 | WAN2-Broadband | wan | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port25 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port26 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port27 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port28 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port29 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port30 |  | lan | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port31 | (ISFW) | lan | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port32 |  | lan | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port33 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port34 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port35 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port36 | WAN\_Uplink | wan | physical | 0 | static | 172.30.72.33/255.255.255.0 | up |
| port37 | HA-Link1 | lan | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port38 | HA-Link2 | lan | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port39 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| port40 |  | n/a | physical | 0 | static | 0.0.0.0/0.0.0.0 | up |
| qtn.FortiLink | (Quarantine VLAN) | n/a | vlan | 4093 | static | 10.254.254.254/255.255.255.0 | up |
| snf.FortiLink | (Sniffer VLAN) | n/a | vlan | 4092 | static | 10.254.253.254/255.255.254.0 | up |
| ssl.root | SSL VPN interface | n/a | tunnel | 0 | static | 0.0.0.0/0.0.0.0 | up |
| test |  | lan | vlan | 100 | static | 0.0.0.0/0.0.0.0 | up |
| voi.FortiLink | (Fortivoice VLAN) | n/a | vlan | 4091 | static | 0.0.0.0/0.0.0.0 | up |
| vsw.FortiLink |  | n/a | vlan | 1 | static | 0.0.0.0/0.0.0.0 | up |

Table - Interface

## 1.3 Route

The following section details route settings configured on FortiGate.

### 1.3.1 Summary

The following section provides a summary of route settings.

|  |  |
| --- | --- |
| Monitor Route | 28 |
| Static Route | 12 |
| 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 | 10.10.1.0/24 | 0.0.0.0 | FortiSASE | 0 / 0 / 0 |
| connect | 10.10.1.1/32 | 0.0.0.0 | FortiSASE | 0 / 0 / 0 |
| 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 | 20 / 0 / 1 |
| enable | VPN-GCP\_remote | 34.125.159.157 | VPN-GCP | 10 / 0 / 1 |
| enable | VPN-SDB\_remote | 96.45.34.228 | VPN-SDB | 10 / 0 / 1 |

Table - Static Route

## 1.4 SD-WAN

The following section details SD-WAN settings configured on FortiGate.

### 1.4.1 Summary

The following section provides a summary of SD-WAN settings.

|  |  |
| --- | --- |
| Zone | 1 |
| Member | 0 |
| Health Check | 0 |
| Rules | 0 |

Table - Summary

### 1.4.2 Configuration

The following section provides configuration of SD-WAN settings.

|  |  |
| --- | --- |
| Status | disable |
| Load Balance Mode | source-ip-based |
| Neighbor Hold Down | disable |
| Fail Detect | disable |

Table - Configuration

### 1.4.3 SD-WAN Zone

| Name | Service SLA |
| --- | --- |
| virtual-wan-link | cfg-order |

Table - SD-WAN Zone

## 1.5 Firewall

The following section details firewall settings configured on FortiGate.

### 1.5.1 Summary

The following section provides a summary of firewall settings.

|  |  |
| --- | --- |
| Address | 86 (Not use: 56 / 65.12%) |
| Group | 9 (Not use: 1 / 11.11%) |
| IP Pool | 1 (Not use: 0 / 0%) |
| Virtual IP | 16 (Not use: 0 / 0%) |
| Policy | 29 (Disabled: 0) |

Table - Summary

### 1.5.2 Address

| Name | Type | Value | Interface | Comment | ref |
| --- | --- | --- | --- | --- | --- |
| 10.100.10.0 | ipmask | 255.255.255.0/255.255.255.255 |  |  | 1 |
| 104.100.76.98@2024-02-28\_08:41:13 | ipmask | 104.100.76.98/255.255.255.255 |  | autocreated at 2024-02-28 08:41:13 | 1 |
| 192.168.20.2@2024-02-28\_08:41:13 | ipmask | 192.168.20.2/255.255.255.255 |  | autocreated at 2024-02-28 08:41:13 | 1 |
| Cloud\_FAP-Eng | ipmask | 10.88.110.201/255.255.255.255 | FortiLink |  | 1 |
| Cloud\_FAP-Fin | ipmask | 10.88.120.200/255.255.255.255 | FortiLink |  | 1 |
| Cloud\_FAP-Sales | ipmask | 10.88.130.154/255.255.255.255 | FortiLink |  | 1 |
| DCFW address | interface-subnet | 10.88.130.154/255.255.255.255 |  |  | 0 |
| EMS1\_ZTNA\_EDR-Classification | dynamic | 10.88.130.154/255.255.255.255 |  |  | 0 |
| EMS1\_ZTNA\_Endpoint\_Compliance | dynamic | 10.88.130.154/255.255.255.255 |  |  | 0 |
| EMS1\_ZTNA\_Important | dynamic | 10.88.130.154/255.255.255.255 |  |  | 0 |
| EMS1\_ZTNA\_Infected | dynamic | 10.88.130.154/255.255.255.255 |  |  | 0 |
| EMS1\_ZTNA\_TEST | dynamic | 10.88.130.154/255.255.255.255 |  |  | 0 |
| EMS1\_ZTNA\_Vulnerable | dynamic | 10.88.130.154/255.255.255.255 |  |  | 0 |
| EMS1\_ZTNA\_Windows 10 | dynamic | 10.88.130.154/255.255.255.255 |  |  | 0 |
| EMS1\_ZTNA\_all\_registered\_clients | dynamic | 10.88.130.154/255.255.255.255 |  |  | 0 |
| EMS1\_ZTNA\_noav | dynamic | 10.88.130.154/255.255.255.255 |  |  | 0 |
| EMS1\_ZTNA\_nos | dynamic | 10.88.130.154/255.255.255.255 |  |  | 0 |
| EMS\_ALL\_UNKNOWN\_CLIENTS | dynamic | 10.88.130.154/255.255.255.255 |  |  | 0 |
| EMS\_ALL\_UNMANAGEABLE\_CLIENTS | dynamic | 10.88.130.154/255.255.255.255 |  |  | 0 |
| FABRIC\_DEVICE | ipmask | 0.0.0.0/0.0.0.0 |  | IPv4 addresses of Fabric Devices. | 0 |
| FAP-Eng | ipmask | 10.88.110.201/255.255.255.255 | FortiLink |  | 1 |
| FAP-Fin | ipmask | 10.88.120.200/255.255.255.255 | FortiLink |  | 1 |
| FCTEMS0000099518\_Critical | dynamic | 10.88.120.200/255.255.255.255 |  |  | 0 |
| FCTEMS0000099518\_EDR-Classification | dynamic | 10.88.120.200/255.255.255.255 |  |  | 0 |
| FCTEMS0000099518\_Finance | dynamic | 10.88.120.200/255.255.255.255 |  |  | 0 |
| FCTEMS0000099518\_High | dynamic | 10.88.120.200/255.255.255.255 |  |  | 0 |
| FCTEMS0000099518\_Important | dynamic | 10.88.120.200/255.255.255.255 |  |  | 0 |
| FCTEMS0000099518\_Infected | dynamic | 10.88.120.200/255.255.255.255 |  |  | 0 |
| FCTEMS0000099518\_Low | dynamic | 10.88.120.200/255.255.255.255 |  |  | 0 |
| FCTEMS0000099518\_Medium | dynamic | 10.88.120.200/255.255.255.255 |  |  | 0 |
| FCTEMS0000099518\_TEST | dynamic | 10.88.120.200/255.255.255.255 |  |  | 0 |
| FCTEMS0000099518\_Windows 10 | dynamic | 10.88.120.200/255.255.255.255 |  |  | 0 |
| FCTEMS0000099518\_all\_registered\_clients | dynamic | 10.88.120.200/255.255.255.255 |  |  | 0 |
| FCTEMS0000099518\_noav | dynamic | 10.88.120.200/255.255.255.255 |  |  | 0 |
| FCTEMS0000099518\_nos | dynamic | 10.88.120.200/255.255.255.255 |  |  | 0 |
| FCTEMS0000099518\_test | dynamic | 10.88.120.200/255.255.255.255 |  |  | 0 |
| FCTEMS\_ALL\_FORTICLOUD\_SERVERS | dynamic | 10.88.120.200/255.255.255.255 |  |  | 0 |
| FIREWALL\_AUTH\_PORTAL\_ADDRESS | ipmask | 0.0.0.0/0.0.0.0 |  |  | 0 |
| FSA-Admin-sw | ipmask | 10.88.23.8/255.255.255.255 | FSA-DMZ |  | 1 |
| FortiEDR\_54.73.53.134 | iprange | 10.88.23.8/255.255.255.255 |  | FortiEDR Event ID - 9174845 | 1 |
| FortiEDR\_54.161.222.85 | iprange | 10.88.23.8/255.255.255.255 |  | FortiEDR Event ID - 8854467 | 1 |
| FortiEDR\_74.125.34.46 | iprange | 10.88.23.8/255.255.255.255 |  | FortiEDR Event ID - 10722934 | 1 |
| FortiEDR\_142.4.205.47 | iprange | 10.88.23.8/255.255.255.255 |  | FortiEDR Event ID - 105864 | 1 |
| FortiEDR\_166.1.173.27 | iprange | 10.88.23.8/255.255.255.255 |  | FortiEDR Event ID - 11597021 | 1 |
| FortiEDR\_188.114.96.7 | iprange | 10.88.23.8/255.255.255.255 |  | FortiEDR Event ID - 9174822 | 1 |
| FortiSASE\_local\_subnet\_1 | ipmask | 10.88.2.0/255.255.255.0 |  |  | 1 |
| ISFW-HA address | interface-subnet | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_EMS1\_ZTNA\_EDR-Classification | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_EMS1\_ZTNA\_Endpoint\_Compliance | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_EMS1\_ZTNA\_Important | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_EMS1\_ZTNA\_Infected | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_EMS1\_ZTNA\_TEST | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_EMS1\_ZTNA\_Vulnerable | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_EMS1\_ZTNA\_Windows 10 | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_EMS1\_ZTNA\_all\_registered\_clients | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_EMS1\_ZTNA\_noav | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_EMS1\_ZTNA\_nos | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_FCTEMS0000099518\_Critical | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_FCTEMS0000099518\_EDR-Classification | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_FCTEMS0000099518\_Finance | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_FCTEMS0000099518\_High | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_FCTEMS0000099518\_Important | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_FCTEMS0000099518\_Infected | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_FCTEMS0000099518\_Low | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_FCTEMS0000099518\_Medium | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_FCTEMS0000099518\_TEST | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_FCTEMS0000099518\_Windows 10 | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_FCTEMS0000099518\_all\_registered\_clients | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_FCTEMS0000099518\_noav | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_FCTEMS0000099518\_nos | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| MAC\_FCTEMS0000099518\_test | dynamic | 10.88.2.0/255.255.255.0 |  |  | 0 |
| SDB-TX | ipmask | 172.31.112.254/255.255.255.255 |  |  | 1 |
| SSLVPN\_TUNNEL\_ADDR1 | iprange | 172.31.112.254/255.255.255.255 |  |  | 0 |
| VAN\_NAT\_1 | ipmask | 208.91.114.4/255.255.255.255 |  |  | 1 |
| VPN-GCP\_local\_subnet\_1 | ipmask | 10.88.2.0/255.255.255.0 |  |  | 1 |
| VPN-GCP\_local\_subnet\_2 | ipmask | 10.88.210.0/255.255.255.0 |  |  | 1 |
| VPN-GCP\_local\_subnet\_3 | ipmask | 10.88.23.0/255.255.255.0 |  |  | 1 |
| VPN-GCP\_remote\_subnet\_1 | ipmask | 172.31.113.0/255.255.255.0 |  |  | 1 |
| VPN-SDB\_local\_subnet\_1 | ipmask | 10.88.2.0/255.255.255.0 |  |  | 1 |
| VPN-SDB\_local\_subnet\_2 | ipmask | 10.88.210.0/255.255.255.0 |  |  | 1 |
| VPN-SDB\_local\_subnet\_3 | ipmask | 10.88.23.0/255.255.255.0 |  |  | 1 |
| VPN-SDB\_local\_subnet\_4 | ipmask | 172.30.72.0/255.255.255.0 |  |  | 1 |
| VPN-SDB\_remote\_subnet\_1 | ipmask | 172.31.112.0/255.255.255.0 |  |  | 1 |
| all | ipmask | 0.0.0.0/0.0.0.0 |  |  | 40 |
| qtn.mac\_00:00:00:00:00:00 | mac | 0.0.0.0/0.0.0.0 |  | Quarantine dummy MAC to keep the addrgrp | 1 |
| qtn.mac\_1c:69:7a:6c:eb:81 | mac | 0.0.0.0/0.0.0.0 |  | Quarantine MAC | 1 |

Table - Address

### 1.5.3 Address Group

| Name | Member | Comment | Ref |
| --- | --- | --- | --- |
| BAD\_GUYS | VAN\_NAT\_1 |  | 1 |
| FortiEDR\_Malicious\_Destinations |  | Members of this group will be automatically added by FortiEDR | 1 |
| FortiSASE\_local | FortiSASE\_local\_subnet\_1 | VPN: FortiSASE (Created by VPN wizard) | 1 |
| FortiXDR\_Malicious\_Destinations | FortiEDR\_142.4.205.47, FortiEDR\_54.161.222.85, FortiEDR\_188.114.96.7, FortiEDR\_54.73.53.134, FortiEDR\_74.125.34.46, FortiEDR\_166.1.173.27 |  | 1 |
| QuarantinedDevices | qtn.mac\_00:00:00:00:00:00, qtn.mac\_1c:69:7a:6c:eb:81 |  | 0 |
| VPN-GCP\_local | VPN-GCP\_local\_subnet\_1, VPN-GCP\_local\_subnet\_2, VPN-GCP\_local\_subnet\_3 | VPN: VPN-GCP (Created by VPN wizard) | 3 |
| VPN-GCP\_remote | VPN-GCP\_remote\_subnet\_1 | VPN: VPN-GCP (Created by VPN wizard) | 4 |
| VPN-SDB\_local | VPN-SDB\_local\_subnet\_1, VPN-SDB\_local\_subnet\_2, VPN-SDB\_local\_subnet\_3, VPN-SDB\_local\_subnet\_4 | VPN: VPN-SDB (Created by VPN wizard) | 3 |
| VPN-SDB\_remote | VPN-SDB\_remote\_subnet\_1 | VPN: VPN-SDB (Created by VPN wizard) | 4 |

Table - Address Group

### 1.5.4 IP Pool

| Name | Interface | Type | Start IP | End IP | Source Start IP | Source End IP | Comments | Ref |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| FSAport3 |  | overload | 172.30.72.105 | 172.30.72.105 | 0.0.0.0 | 0.0.0.0 |  | 1 |

Table - Virtual IP

### 1.5.5 Virtual IP

| Name | Interface | External IP | Mapped IP | Protocol | External Port | Mapped Port | Comment | Ref |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| FortiSandbox-VIP | port36 | 172.30.72.80 | 10.88.23.8 | tcp | 0-65535 | 0-65535 |  | 1 |
| FortiMail IBE | port36 | 172.30.72.176 | 10.88.11.1 | tcp | 0-65535 | 0-65535 |  | 1 |
| FortiGate-DCFW | port36 | 172.30.72.154 | 10.88.2.21 | tcp | 0-65535 | 0-65535 |  | 1 |
| FortiSandbox-Slave-IP | port36 | 172.30.72.79 | 10.88.23.9 | tcp | 0-65535 | 0-65535 |  | 1 |
| WLC VIP | port36 | 172.30.72.40 | 10.88.51.1 | tcp | 0-65535 | 0-65535 |  | 1 |
| FCTEMS\_FWB | port36 | 172.30.72.106 | 10.88.210.101 | tcp | 0-65535 | 0-65535 |  | 1 |
| FSIEM\_VIP | port36 | 172.30.72.244 | 10.88.210.32 | tcp | 0-65535 | 0-65535 |  | 1 |
| WLM\_VIP | port36 | 172.30.72.41 | 10.88.51.2 | tcp | 0-65535 | 0-65535 |  | 2 |
| FortiNAC | port36 | 172.30.72.43 | 10.88.210.50 | tcp | 0-65535 | 0-65535 |  | 1 |
| FAC | port36 | 172.30.72.247 | 10.88.210.163 | tcp | 0-65535 | 0-65535 |  | 1 |
| FortiManager | port36 | 172.30.72.239 | 10.88.210.253 | tcp | 0-65535 | 0-65535 |  | 1 |
| FortiAnalyzer | port36 | 172.30.72.62 | 10.88.210.62 | tcp | 0-65535 | 0-65535 |  | 1 |
| LANEdge-VIP | port36 | 172.30.72.156 | 10.88.12.99 | tcp | 0-65535 | 0-65535 |  | 2 |
| FortiAP-VIP ISFW-E | port36 | 172.30.72.157 | 10.88.101.99 | tcp | 0-65535 | 0-65535 |  | 2 |
| ISFW\_BLDG-F | port36 | 172.30.72.158 | 10.88.120.254 | tcp | 0-65535 | 0-65535 |  | 1 |
| ISFW\_BLDG-B | port36 | 172.30.72.159 | 10.88.130.254 | tcp | 0-65535 | 0-65535 |  | 1 |

Table - Virtual IP

### 1.5.6 Policy Summary

The following section provides a policy summary of firewall settings.

|  |  |
| --- | --- |
| Policy | 29 |
| Enabled | 29 (100%) |
| Deny | 1 (3.45%) |
| NAT | 13 (44.83%) |
| Logging | All: 22 (75.86%) UTM: 7 (24.14%) Disable: 0 (0%) |
| Unnamed | 1 (3.45%) |
| Comments | 13 (44.83%) |
| SSH/SSH Inspection | 8 (27.59%) |

Table - Policy Summary

### 1.5.7 Policy

### 1.5.7.1 Policy - Normal

| 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 |  |
|  | port4 | port36 | 192.168.20.2@2024-02-28\_08:41:13 | 104.100.76.98@2024-02-28\_08:41:13 | HTTP | accept | enable | all | autocreated at 2024-02-28 08:41:13 |
| 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 | all |  |
| ISFW-FSA | ISFW-HA, DCFW | FSA-DMZ | all | all | ALL | accept | enable | all |  |
| Wireless-WLC | WLC-Students, WLC-Staff, WLC-Teachers, FWLC | port36 | all | all | ALL | accept | enable | all |  |
| IS-DC | ISFW-HA, FWLC, WLC-Staff, WLC-Students, WLC-Teachers | DCFW, ISFW-HA | all | all | ALL | accept | disable | all |  |
| DC-IS | DCFW, ISFW-HA | ISFW-HA, FWLC, WLC-Staff, WLC-Students, WLC-Teachers | all | all | ALL | accept | enable | 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 to DCFW\_VIP NAT | port36 | DCFW | SDB-TX | FGT\_DCFW\_VIPG | ALL | accept | enable | all | (Copy of WAN\_DCFW\_VIP) |
| 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) |
| WAN\_ISFWs\_VIP | port36 | ISFW-HA | all | ISFW\_BLDG-F, ISFW\_BLDG-B, FortiAP-VIP ISFW-E, LANEdge-VIP | ALL | accept | disable | all | (Copy of WAN\_DCFW\_VIP) (Copy of WAN\_ISFW-E\_VIP) (Copy of WAN\_ISFW-F\_VIP) |
| WAN\_FortiAP-VIP ISFW-E\_VIP | port36 | ISFW-HA | all | FortiAP-VIP ISFW-E | ALL | accept | disable | all | (Copy of WAN\_DCFW\_VIP) |
| Allow-DNS | any | any | all | all | SYSLOG | accept | enable | all |  |
| vpn\_VPN-GCP\_local\_0 | DCFW | VPN-GCP | VPN-GCP\_local | VPN-GCP\_remote | ALL | accept | disable | utm | VPN: VPN-GCP (Created by VPN wizard) |
| vpn\_VPN-GCP\_remote\_0 | VPN-GCP | any | VPN-GCP\_remote | VPN-GCP\_local | ALL | accept | enable | all | VPN: VPN-GCP (Created by VPN wizard) |
| vpn\_VPN-SDB\_local\_0 | DCFW | VPN-SDB | VPN-SDB\_local | VPN-SDB\_remote | ALL | accept | disable | utm | VPN: VPN-SDB (Created by VPN wizard) |
| vpn\_VPN-SDB\_remote\_0 | VPN-SDB | any | VPN-SDB\_remote | VPN-SDB\_local | ALL | accept | enable | all | VPN: VPN-SDB (Created by VPN wizard) |
| Policyin | any | any | all | all | ALL | accept | disable | all |  |
| vpn\_FortiSASE\_spoke2hub\_0 | FortiSASE | DCFW | all | FortiSASE\_local | ALL | accept | disable | utm | VPN: FortiSASE (Created by VPN wizard) |
| vpn\_FortiSASE\_spoke2spoke\_0 | FortiSASE | FortiSASE | all | all | ALL | accept | disable | utm | VPN: FortiSASE (Created by VPN wizard) |
| Guest | port16 | port36 | all | all | ALL | accept | disable | all |  |

Table - Policy

### 1.5.7.2 Policy - Interface Pair

#### 1.5.7.2.1 Policy: any => any

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| DNS | all | all | SYSLOG, DNS | accept | enable | all |  |
| Allow-DNS | all | all | SYSLOG | accept | enable | all |  |
| Policyin | all | all | ALL | accept | disable | all |  |

Table - Policy - any => any

#### 1.5.7.2.2 Policy: DCFW => FSA-DMZ

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ISFW-FSA | all | all | ALL | accept | enable | all |  |

Table - Policy - DCFW => FSA-DMZ

#### 1.5.7.2.3 Policy: DCFW => FWLC

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| DC-IS | all | all | ALL | accept | enable | all | Reverse of ISFW-DCFW |

Table - Policy - DCFW => FWLC

#### 1.5.7.2.4 Policy: DCFW => ISFW-HA

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| DC-IS | all | all | ALL | accept | enable | all | Reverse of ISFW-DCFW |

Table - Policy - DCFW => ISFW-HA

#### 1.5.7.2.5 Policy: DCFW => port36

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Block Malicious by FortiEDR | all | FortiEDR\_Malicious\_Destinations, FortiXDR\_Malicious\_Destinations | ALL | deny | disable | all |  |
| ISFW-WAN | all | all | ALL | accept | enable | all | Skip ISFWs will Scan |

Table - Policy - DCFW => port36

#### 1.5.7.2.6 Policy: DCFW => VPN-GCP

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| vpn\_VPN-GCP\_local\_0 | VPN-GCP\_local | VPN-GCP\_remote | ALL | accept | disable | utm | VPN: VPN-GCP (Created by VPN wizard) |

Table - Policy - DCFW => VPN-GCP

#### 1.5.7.2.7 Policy: DCFW => VPN-SDB

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| vpn\_VPN-SDB\_local\_0 | VPN-SDB\_local | VPN-SDB\_remote | ALL | accept | disable | utm | VPN: VPN-SDB (Created by VPN wizard) |

Table - Policy - DCFW => VPN-SDB

#### 1.5.7.2.8 Policy: DCFW => WLC-Staff

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| DC-IS | all | all | ALL | accept | enable | all | Reverse of ISFW-DCFW |

Table - Policy - DCFW => WLC-Staff

#### 1.5.7.2.9 Policy: DCFW => WLC-Students

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| DC-IS | all | all | ALL | accept | enable | all | Reverse of ISFW-DCFW |

Table - Policy - DCFW => WLC-Students

#### 1.5.7.2.10 Policy: DCFW => WLC-Teachers

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| DC-IS | all | all | ALL | accept | enable | all | Reverse of ISFW-DCFW |

Table - Policy - DCFW => WLC-Teachers

#### 1.5.7.2.11 Policy: FITNUC => port36

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| FIT - Intel NUC outbound | all | all | ALL | accept | enable | all |  |

Table - Policy - FITNUC => port36

#### 1.5.7.2.12 Policy: FortiSASE => DCFW

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| vpn\_FortiSASE\_spoke2hub\_0 | all | FortiSASE\_local | ALL | accept | disable | utm | VPN: FortiSASE (Created by VPN wizard) |

Table - Policy - FortiSASE => DCFW

#### 1.5.7.2.13 Policy: FortiSASE => FortiSASE

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| vpn\_FortiSASE\_spoke2spoke\_0 | all | all | ALL | accept | disable | utm | VPN: FortiSASE (Created by VPN wizard) |

Table - Policy - FortiSASE => FortiSASE

#### 1.5.7.2.14 Policy: FSA-DMZ => port36

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Allow FSA Access | FSA-Admin-sw | all | ALL | accept | enable | utm |  |

Table - Policy - FSA-DMZ => port36

#### 1.5.7.2.15 Policy: FSA-DMZ2 => port36

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| FSA-DMZ-WAN | all | all | ALL | accept | enable | all |  |

Table - Policy - FSA-DMZ2 => port36

#### 1.5.7.2.16 Policy: FWLC => DCFW

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| IS-DC | all | all | ALL | accept | disable | all |  |

Table - Policy - FWLC => DCFW

#### 1.5.7.2.17 Policy: FWLC => ISFW-HA

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| IS-DC | all | all | ALL | accept | disable | all |  |

Table - Policy - FWLC => ISFW-HA

#### 1.5.7.2.18 Policy: FWLC => port36

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Block Malicious by FortiEDR | all | FortiEDR\_Malicious\_Destinations, FortiXDR\_Malicious\_Destinations | ALL | deny | disable | all |  |
| Wireless-WLC | all | all | ALL | accept | enable | all |  |

Table - Policy - FWLC => port36

#### 1.5.7.2.19 Policy: ISFW-HA => DCFW

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| IS-DC | all | all | ALL | accept | disable | all |  |

Table - Policy - ISFW-HA => DCFW

#### 1.5.7.2.20 Policy: ISFW-HA => FSA-DMZ

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ISFW-FSA | all | all | ALL | accept | enable | all |  |

Table - Policy - ISFW-HA => FSA-DMZ

#### 1.5.7.2.21 Policy: ISFW-HA => FWLC

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| DC-IS | all | all | ALL | accept | enable | all | Reverse of ISFW-DCFW |

Table - Policy - ISFW-HA => FWLC

#### 1.5.7.2.22 Policy: ISFW-HA => ISFW-HA

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| IS-DC | all | all | ALL | accept | disable | all |  |
| DC-IS | all | all | ALL | accept | enable | all | Reverse of ISFW-DCFW |

Table - Policy - ISFW-HA => ISFW-HA

#### 1.5.7.2.23 Policy: ISFW-HA => port36

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Block Malicious by FortiEDR | all | FortiEDR\_Malicious\_Destinations, FortiXDR\_Malicious\_Destinations | ALL | deny | disable | all |  |
| ISFW-WAN | all | all | ALL | accept | enable | all | Skip ISFWs will Scan |

Table - Policy - ISFW-HA => port36

#### 1.5.7.2.24 Policy: ISFW-HA => WLC-Staff

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| DC-IS | all | all | ALL | accept | enable | all | Reverse of ISFW-DCFW |

Table - Policy - ISFW-HA => WLC-Staff

#### 1.5.7.2.25 Policy: ISFW-HA => WLC-Students

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| DC-IS | all | all | ALL | accept | enable | all | Reverse of ISFW-DCFW |

Table - Policy - ISFW-HA => WLC-Students

#### 1.5.7.2.26 Policy: ISFW-HA => WLC-Teachers

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| DC-IS | all | all | ALL | accept | enable | all | Reverse of ISFW-DCFW |

Table - Policy - ISFW-HA => WLC-Teachers

#### 1.5.7.2.27 Policy: P22 => port36

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| IBE-WAN | all | all | ALL | accept | disable | utm |  |

Table - Policy - P22 => port36

#### 1.5.7.2.28 Policy: port16 => port36

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Guest | all | all | ALL | accept | disable | all |  |

Table - Policy - port16 => port36

#### 1.5.7.2.29 Policy: port36 => DCFW

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| WAN to DCFW\_VIP NAT | SDB-TX | FGT\_DCFW\_VIPG | ALL | accept | enable | all | (Copy of WAN\_DCFW\_VIP) |
| WAN\_DCFW\_VIP | all | FGT\_DCFW\_VIPG | ALL | accept | disable | all |  |

Table - Policy - port36 => DCFW

#### 1.5.7.2.30 Policy: port36 => FSA-DMZ

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| FSA-MGMT-VIP | all | FortiSandbox-VIP, FortiSandbox-Slave-IP | ALL\_ICMP, HTTP, HTTPS, OFTP, SSH, RADIUS | accept | disable | all |  |

Table - Policy - port36 => FSA-DMZ

#### 1.5.7.2.31 Policy: port36 => FWLC

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| WAN-FWLC-VIP | all | WLC VIP, WLM\_VIP | ALL | accept | disable | all |  |

Table - Policy - port36 => FWLC

#### 1.5.7.2.32 Policy: port36 => ISFW-HA

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| WAN\_ISFW\_VIP | all | LANEdge-VIP | ALL | accept | disable | all | (Copy of WAN\_DCFW\_VIP) |
| WAN\_ISFWs\_VIP | all | ISFW\_BLDG-F, ISFW\_BLDG-B, FortiAP-VIP ISFW-E, LANEdge-VIP | ALL | accept | disable | all | (Copy of WAN\_DCFW\_VIP) (Copy of WAN\_ISFW-E\_VIP) (Copy of WAN\_ISFW-F\_VIP) |
| WAN\_FortiAP-VIP ISFW-E\_VIP | all | FortiAP-VIP ISFW-E | ALL | accept | disable | all | (Copy of WAN\_DCFW\_VIP) |

Table - Policy - port36 => ISFW-HA

#### 1.5.7.2.33 Policy: port36 => P22

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| WAN-IBE | all | FortiMail IBE | ALL | accept | disable | utm |  |

Table - Policy - port36 => P22

#### 1.5.7.2.34 Policy: port36 => WLC-Staff

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| WAN-FWLC-VIP | all | WLC VIP, WLM\_VIP | ALL | accept | disable | all |  |

Table - Policy - port36 => WLC-Staff

#### 1.5.7.2.35 Policy: port36 => WLC-Students

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| WAN-FWLC-VIP | all | WLC VIP, WLM\_VIP | ALL | accept | disable | all |  |

Table - Policy - port36 => WLC-Students

#### 1.5.7.2.36 Policy: port36 => WLC-Teachers

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| WAN-FWLC-VIP | all | WLC VIP, WLM\_VIP | ALL | accept | disable | all |  |

Table - Policy - port36 => WLC-Teachers

#### 1.5.7.2.37 Policy: port4 => port36

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 192.168.20.2@2024-02-28\_08:41:13 | 104.100.76.98@2024-02-28\_08:41:13 | HTTP | accept | enable | all | autocreated at 2024-02-28 08:41:13 |
| FIT - Intel NUC outbound | all | all | ALL | accept | enable | all |  |

Table - Policy - port4 => port36

#### 1.5.7.2.38 Policy: VPN-GCP => any

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| vpn\_VPN-GCP\_remote\_0 | VPN-GCP\_remote | VPN-GCP\_local | ALL | accept | enable | all | VPN: VPN-GCP (Created by VPN wizard) |

Table - Policy - VPN-GCP => any

#### 1.5.7.2.39 Policy: VPN-SDB => any

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| vpn\_VPN-SDB\_remote\_0 | VPN-SDB\_remote | VPN-SDB\_local | ALL | accept | enable | all | VPN: VPN-SDB (Created by VPN wizard) |

Table - Policy - VPN-SDB => any

#### 1.5.7.2.40 Policy: WLC-Staff => DCFW

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| IS-DC | all | all | ALL | accept | disable | all |  |

Table - Policy - WLC-Staff => DCFW

#### 1.5.7.2.41 Policy: WLC-Staff => ISFW-HA

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| IS-DC | all | all | ALL | accept | disable | all |  |

Table - Policy - WLC-Staff => ISFW-HA

#### 1.5.7.2.42 Policy: WLC-Staff => port36

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Block Malicious by FortiEDR | all | FortiEDR\_Malicious\_Destinations, FortiXDR\_Malicious\_Destinations | ALL | deny | disable | all |  |
| Wireless-WLC | all | all | ALL | accept | enable | all |  |

Table - Policy - WLC-Staff => port36

#### 1.5.7.2.43 Policy: WLC-Students => DCFW

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| IS-DC | all | all | ALL | accept | disable | all |  |

Table - Policy - WLC-Students => DCFW

#### 1.5.7.2.44 Policy: WLC-Students => ISFW-HA

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| IS-DC | all | all | ALL | accept | disable | all |  |

Table - Policy - WLC-Students => ISFW-HA

#### 1.5.7.2.45 Policy: WLC-Students => port36

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Block Malicious by FortiEDR | all | FortiEDR\_Malicious\_Destinations, FortiXDR\_Malicious\_Destinations | ALL | deny | disable | all |  |
| Wireless-WLC | all | all | ALL | accept | enable | all |  |

Table - Policy - WLC-Students => port36

#### 1.5.7.2.46 Policy: WLC-Teachers => DCFW

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| IS-DC | all | all | ALL | accept | disable | all |  |

Table - Policy - WLC-Teachers => DCFW

#### 1.5.7.2.47 Policy: WLC-Teachers => ISFW-HA

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| IS-DC | all | all | ALL | accept | disable | all |  |

Table - Policy - WLC-Teachers => ISFW-HA

#### 1.5.7.2.48 Policy: WLC-Teachers => port36

| Name | Source | Destination | Service | Action | NAT | Log | Comments |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Block Malicious by FortiEDR | all | FortiEDR\_Malicious\_Destinations, FortiXDR\_Malicious\_Destinations | ALL | deny | disable | all |  |
| Wireless-WLC | all | all | ALL | accept | enable | all |  |

Table - Policy - WLC-Teachers => port36

## 1.6 User

The following section details user settings configured on FortiGate.

### 1.6.1 Summary

The following section provides a summary of user settings.

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

Table - Summary

### 1.6.2 User Group

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

Table - User Group

### 1.6.3 LDAP

| Name | Server(s) | 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

LDAP: ad-fortidemo

|  |  |
| --- | --- |
| Name | ad-fortidemo |
| Server | 10.88.210.100 |
| Secondary Server |  |
| Tertiary Server |  |
| Port | 389 |
| Secure | disable |
| Source IP | 0.0.0.0 |
| Interface |  |
| Cnid | sAMAccountName |
| DN | dc=corp,dc=fortidemo,dc=com |
| Type | regular |
| Username | administrator@corp.fortidemo.com |
| Group Member Check | user-attr |
| Group Search Base |  |
| Group Object Filter | (&(objectcategory=group)(member=\*)) |

Table - LDAP ad-fortidemo

### 1.6.4 RADIUS

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

Table - RADIUS

RADIUS: FAC-DEMO

|  |  |
| --- | --- |
| Name | FAC-DEMO |
| Server | 172.30.72.232 |
| Secondary Server | 172.30.72.231 |
| Tertiary Server |  |
| Port | 0 |
| Timeout | 5 |
| Source IP |  |
| Interface |  |
| Interface Select Method | auto |
| Use Management VDOM | disable |
| All Usergroup | disable |
| NAS IP | 0.0.0.0 |
| NAS ID Type | legacy |
| NAS ID |  |
| Acct Interim Interval | 0 |
| RADIUS CoA | disable |
| Auth Type | auto |
| Username Case Sensitive | disable |
| Accounting Server |  |
| RSSO | disable |
| Class |  |
| Password Renewal | disable |
| MAC Username Delimiter | hyphen |
| MAC Password Delimiter |  |
| MAC Case | lowercase |
| Delimiter | plus |

Table - RADIUS FAC-DEMO

## 1.7 VPN IPsec

The following section details VPN IPsec settings configured on FortiGate.

### 1.7.1 Summary

The following section provides a summary of VPN IPsec settings.

|  |  |
| --- | --- |
| VPN IPsec Phase 1 | 4 |
| VPN IPsec Phase 2 | 3 |

Table - Summary

### 1.7.2 VPN IPsec Phase 1

Summary

| Name | Type | Interface | Remote Gateway | Mode | Auth method |
| --- | --- | --- | --- | --- | --- |
| FortiSASE | dynamic | port36 | 0.0.0.0 | main | psk |
| VPN-GCP | static | port36 | 34.125.159.157 | main | psk |
| VPN-MPLS1 | dynamic | port23 | 0.0.0.0 | main | psk |
| VPN-SDB | static | port36 | 96.45.34.228 | main | psk |

Table - VPN IPsec Phase 1 Summary

### 1.7.2.1 Phase 1: FortiSASE

|  |  |
| --- | --- |
| Name | FortiSASE |
| Type | dynamic |
| Interface | port36 |
| IP Version | 4 |
| IKE Version | 1 |
| Local Gateway | 0.0.0.0 |
| Remote Gateway | 0.0.0.0 |
| Mode | main |
| Auth method | psk |
| Peer Type | any |
| Comments | VPN: FortiSASE (Created by VPN wizard) |
| Mode CFG | disable |
| Proposal | aes128-sha256, aes256-sha256, aes128-sha1, aes256-sha1 |
| DH Group | 14, 5 |
| Local ID |  |
| DPD | on-idle |
| xAuth Type | disable |
| NAT Traversal | enable |
| Rekey | enable |

Table - VPN IPsec Phase 1: FortiSASE

### 1.7.2.2 Phase 1: VPN-GCP

|  |  |
| --- | --- |
| Name | VPN-GCP |
| Type | static |
| Interface | port36 |
| IP Version | 4 |
| IKE Version | 1 |
| Local Gateway | 0.0.0.0 |
| Remote Gateway | 34.125.159.157 |
| Mode | main |
| Auth method | psk |
| Peer Type | any |
| Comments | VPN: VPN-GCP (Created by VPN wizard) |
| Mode CFG | disable |
| Proposal | aes128-sha256, aes256-sha256, aes128-sha1, aes256-sha1 |
| DH Group | 14, 5 |
| Local ID |  |
| DPD | on-demand |
| xAuth Type | disable |
| NAT Traversal | enable |
| Rekey | enable |

Table - VPN IPsec Phase 1: VPN-GCP

### 1.7.2.3 Phase 1: VPN-MPLS1

|  |  |
| --- | --- |
| Name | VPN-MPLS1 |
| Type | dynamic |
| Interface | port23 |
| IP Version | 4 |
| IKE Version | 1 |
| Local Gateway | 0.0.0.0 |
| Remote Gateway | 0.0.0.0 |
| Mode | main |
| Auth method | psk |
| Peer Type | any |
| Comments |  |
| Mode CFG | disable |
| Proposal | aes256-sha256 |
| DH Group | 5 |
| Local ID |  |
| DPD | on-idle |
| xAuth Type | disable |
| NAT Traversal | enable |
| Rekey | enable |

Table - VPN IPsec Phase 1: VPN-MPLS1

### 1.7.2.4 Phase 1: VPN-SDB

|  |  |
| --- | --- |
| Name | VPN-SDB |
| Type | static |
| Interface | port36 |
| IP Version | 4 |
| IKE Version | 1 |
| Local Gateway | 0.0.0.0 |
| Remote Gateway | 96.45.34.228 |
| Mode | main |
| Auth method | psk |
| Peer Type | any |
| Comments | VPN: VPN-SDB (Created by VPN wizard) |
| Mode CFG | disable |
| Proposal | aes256-sha256 |
| DH Group | 14, 5 |
| Local ID |  |
| DPD | on-demand |
| xAuth Type | disable |
| NAT Traversal | enable |
| Rekey | enable |

Table - VPN IPsec Phase 1: VPN-SDB

### 1.7.3 VPN IPsec Phase 2

Summary

| Name | Phase 1 Name | Source Address Type | Source Address | Destination Address Type | Destination Address |
| --- | --- | --- | --- | --- | --- |
| FortiSASE | FortiSASE | subnet | 0.0.0.0/0.0.0.0 | subnet | 0.0.0.0/0.0.0.0 |
| VPN-GCP | VPN-GCP | name | VPN-GCP\_local | name | VPN-GCP\_remote |
| VPN-SDB | VPN-SDB | name | VPN-SDB\_local | name | VPN-SDB\_remote |

Table - VPN IPsec Phase 1 Summary

### 1.7.3.1 Phase 2: FortiSASE (FortiSASE)

|  |  |
| --- | --- |
| Name | FortiSASE |
| Phase 1 Name | FortiSASE |
| Commnets | VPN: FortiSASE (Created by VPN wizard) |
| Proposal | aes128-sha1, aes256-sha1, aes128-sha256, aes256-sha256, aes128gcm, aes256gcm, chacha20poly1305 |
| DH Group | 14, 5 |
| Replay | enable |
| KeepAlive | disable |
| Keylife Type | seconds |
| Keylife Seconds | 43200 |
| Keylife Kbs | 5120 |
| Source Address Type | subnet |
| Source Address Name |  |
| Source Address Subnet | 0.0.0.0 0.0.0.0 |
| Destination Address Type | subnet |
| Destination Address Name |  |
| Destination Address Subnet | 0.0.0.0 0.0.0.0 |

Table - VPN IPsec Phase 2: FortiSASE

### 1.7.3.2 Phase 2: VPN-GCP (VPN-GCP)

|  |  |
| --- | --- |
| Name | VPN-GCP |
| Phase 1 Name | VPN-GCP |
| Commnets | VPN: VPN-GCP (Created by VPN wizard) |
| Proposal | aes256-sha256 |
| DH Group | 14, 5 |
| Replay | enable |
| KeepAlive | disable |
| Keylife Type | seconds |
| Keylife Seconds | 43200 |
| Keylife Kbs | 5120 |
| Source Address Type | name |
| Source Address Name | VPN-GCP\_local |
| Source Address Subnet |  |
| Destination Address Type | name |
| Destination Address Name | VPN-GCP\_remote |
| Destination Address Subnet |  |

Table - VPN IPsec Phase 2: VPN-GCP

### 1.7.3.3 Phase 2: VPN-SDB (VPN-SDB)

|  |  |
| --- | --- |
| Name | VPN-SDB |
| Phase 1 Name | VPN-SDB |
| Commnets | VPN: VPN-SDB (Created by VPN wizard) |
| Proposal | aes256-sha256 |
| DH Group | 14, 5 |
| Replay | enable |
| KeepAlive | disable |
| Keylife Type | seconds |
| Keylife Seconds | 43200 |
| Keylife Kbs | 5120 |
| Source Address Type | name |
| Source Address Name | VPN-SDB\_local |
| Source Address Subnet |  |
| Destination Address Type | name |
| Destination Address Name | VPN-SDB\_remote |
| Destination Address Subnet |  |

Table - VPN IPsec Phase 2: VPN-SDB

## 1.8 VPN SSL

The following section details VPN SSL settings configured on FortiGate.

### 1.8.1 Summary

The following section provides a summary of VPN SSL settings.

|  |  |
| --- | --- |
| Portal | 1 |
| User (connected) | 0 |

Table - Summary

### 1.8.2 VPN SSL Settings

|  |  |
| --- | --- |
| Status | enable |
| Port | 443 |
| Source Interface |  |
| Source Address |  |
| Default Portal |  |
| Certificate Server | Fortinet\_Factory |
| Algorithm | high |
| Idle Timeout | 300 |
| Auth Timeout | 28800 |
| Force Two factor Auth | disable |
| Tunnel IP Pool | 10.100.10.0 |
| DNS Suffix |  |
| DNS Server1 | 0.0.0.0 |
| DNS Server2 | 0.0.0.0 |

Table - VPN SSL Settings