Bijlage 1

Technische Documentatie

# Technische informatie

Alle devices in het netwerk worden gekenmerkt door een *hostname*.

Dit document geeft aan welke IP-adressen gehanteerd zijn, hoe de VLAN’s zijn ingericht, welke IOS‑versies op de devices staan geïnstalleerd en wat de systeemaccounts zijn. Het beheer op alle devices kan door de netwerkbeheerder worden uitgevoerd via SSH. Van de verbinding tussen de devices is geen actuele tekening beschikbaar.

## IP-adressen

De volgende IP-adressen zijn aan de devices toegekend.

|  |  |
| --- | --- |
| **Netwerkdevice** | **IP-adres** |
| AS1 | 172.30.0.4/16 |
| AS2 | 172.30.0.5/16 |
| AS3 | 172.30.0.6/16 |
| Core | 172.30.0.2/16 |
| MLS | 172.30.0.1/16 |
| DMZ | 10.20.0.2/16 |
| Edge | 10.0.0.2/30 |
| SW-backbone | 10.20.0.5/16 |

|  |  |
| --- | --- |
| **Server** | **IP-adres** |
| NTP/syslog | 172.30.0.100/16 |
| DHCP | 172.30.0.175/16 |
| HTTP | 10.10.0.100/16 |
| Controller | N.v.t. |
| FTP | 172.30.0.50/16 |
| DNS | 172.30.0.200/16 |
|  |  |
|  |  |

## Verdeling VLAN's

Om het uitvalrisico te beperken, zijn de VLAN’s gelijkmatig over de switches verdeeld. Poort 24 is op alle access-switches vrij gelaten voor de netwerkbeheerder.

|  |  |  |  |
| --- | --- | --- | --- |
| **Switch** | **Accesspoorten** | **VLAN-ID** | **Verbonden met** |
| AS1 t/m AS3 | 1 - 5 | 20 | Logistiek |
| 6 - 10 | 21 | Verkoop |
| 11 - 15 | 22 | HRM |
| 16-20 | 23 | Administratie |
| 21-23 | 99 | Ongebruikt |
| 24 | 30 | Beheer en servers |
| MLS | 1/0/18-24 | 30 | Beheer en servers |

## Systeemaccounts

De volgende systeemaccounts zijn aan de devices toegekend.

|  |  |  |
| --- | --- | --- |
| **Service** | **Gebruikersnaam** | **Wachtwoord** |
| Privileged mode | - | **start** |
| SSH | **admin** | **start** |
| Console | **admin** | **start** |
| FTP-server | **ftp-admin** | **B@ckup-cnfg** |

## IOS-versies

Op alle devices hoort de volgende versie van Cisco IOS geïnstalleerd te zijn.

|  |  |
| --- | --- |
| **Netwerkdevice** | **IOS-versie** |
| AS1 | 12.2(25r) |
| AS2 | 12.2(25r) |
| AS3 | 12.2(25r) |
| Core | 12.1(22) |
| MLS | 16.3.2 |
| DMZ | 15.5 (3)S5 |
| Edge | 15.5 (3)S5 |
| SW-backbone | 12.1(22)EA4 |

### Beheerpolicies

De inrichting van het netwerk moet voldoen aan strikte policies. Deze zijn gecategoriseerd in algemene en securitypolicies.

### Algemeen

1. Netwerkinfrastructuur is volledig gedocumenteerd.
2. Harde reset moet tot herstel leiden.
3. Tijdsynchronisatie via NTP
4. Events worden centraal beheerd.
5. Spanning Tree is actief op alle switches.
6. Verbinding met VLAN 20 mag geen vertraging hebben.
7. IP-adressering volgens vastgesteld nummerplan
8. Voldoende IP-adressen gereserveerd
9. Actuele back-ups beschikbaar van alle devices
10. Monitoring testen (steekproef)
11. IOS-versies zijn up-to-date
12. Voldoende poortcapaciteit beschikbaar
13. Voldoende bandbreedte beschikbaar

### Security

1. Beheer op afstand: uitsluitend SSH
2. Wachtwoorden zijn versleuteld opgeslagen.
3. Ongeautoriseerd netwerk uitbreiden is geblokkeerd.
4. Ongebruikte poorten staan dicht.
5. Man-in-the-middle-beveiliging is geactiveerd (DHCP).
6. Aantal VLAN's per trunk is gelimiteerd tot minimum.
7. VLAN 1 mag niet worden gebruikt.
8. Spanning Tree-proces mag niet door derden beïnvloed worden.
9. Geen autodetectiesoftware actief op switchpoorten
10. VLAN’s zijn onderling van elkaar gescheiden.
11. Routingupdates uitsluitend via aangewezen poorten
12. Toegang tot alle software en devices is beveiligd.