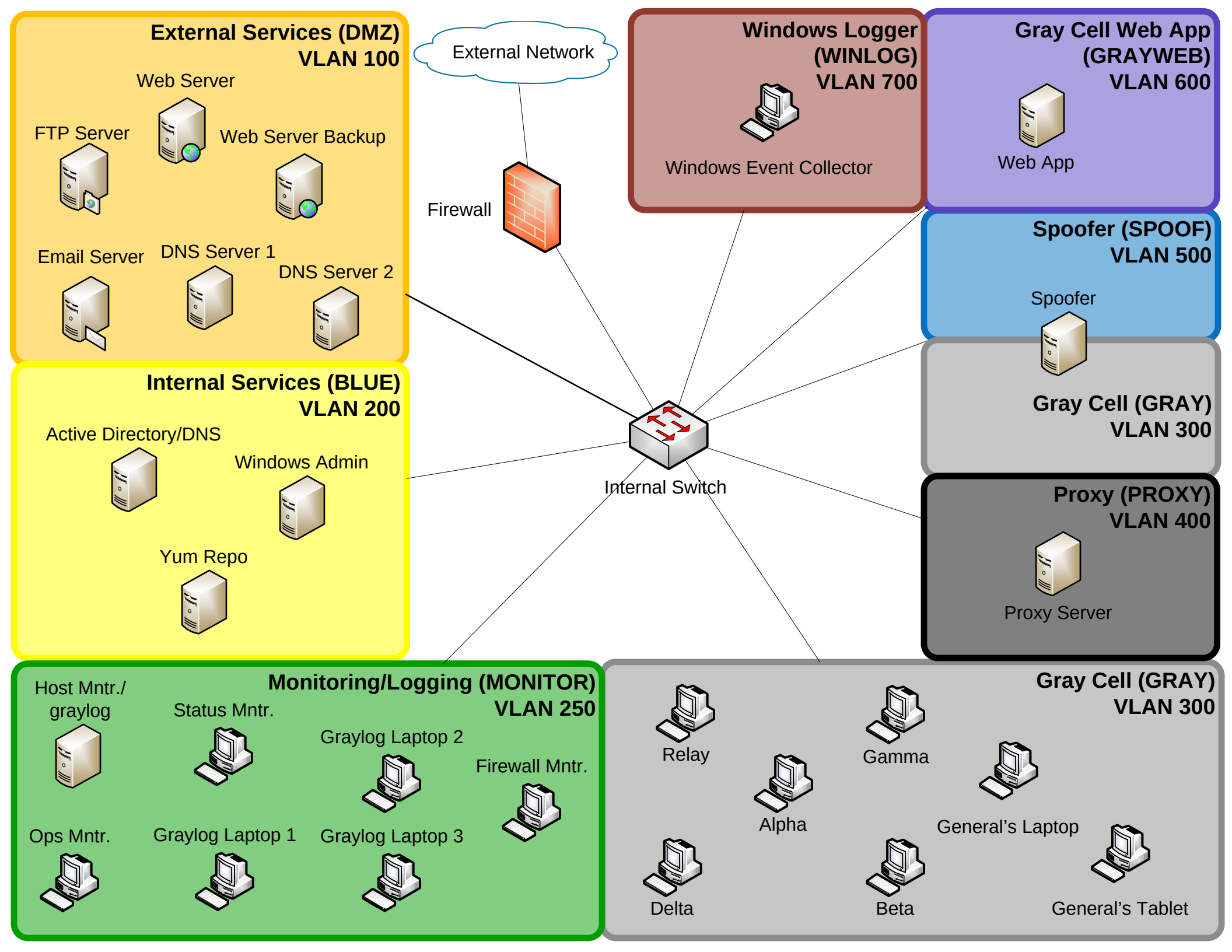
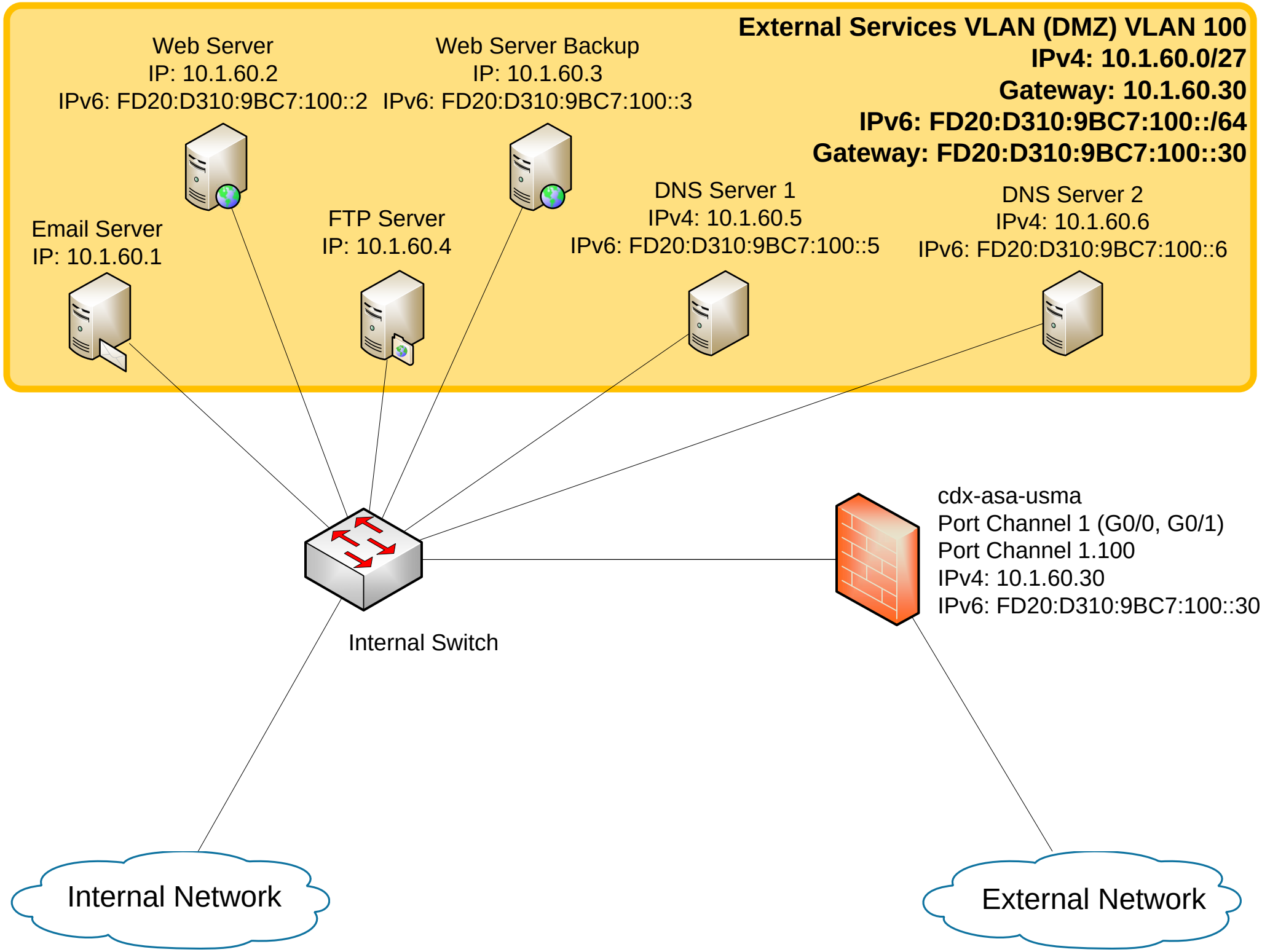
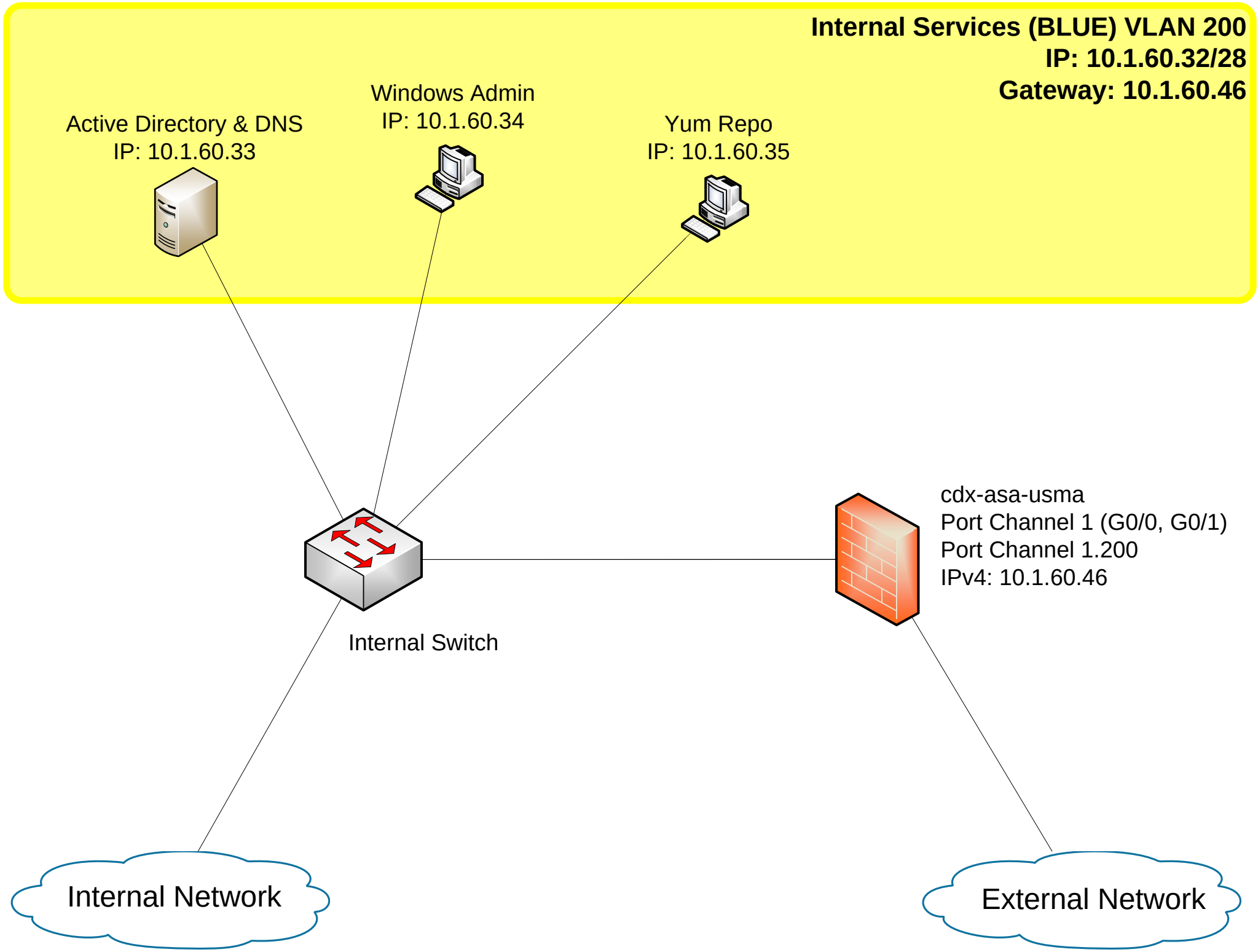
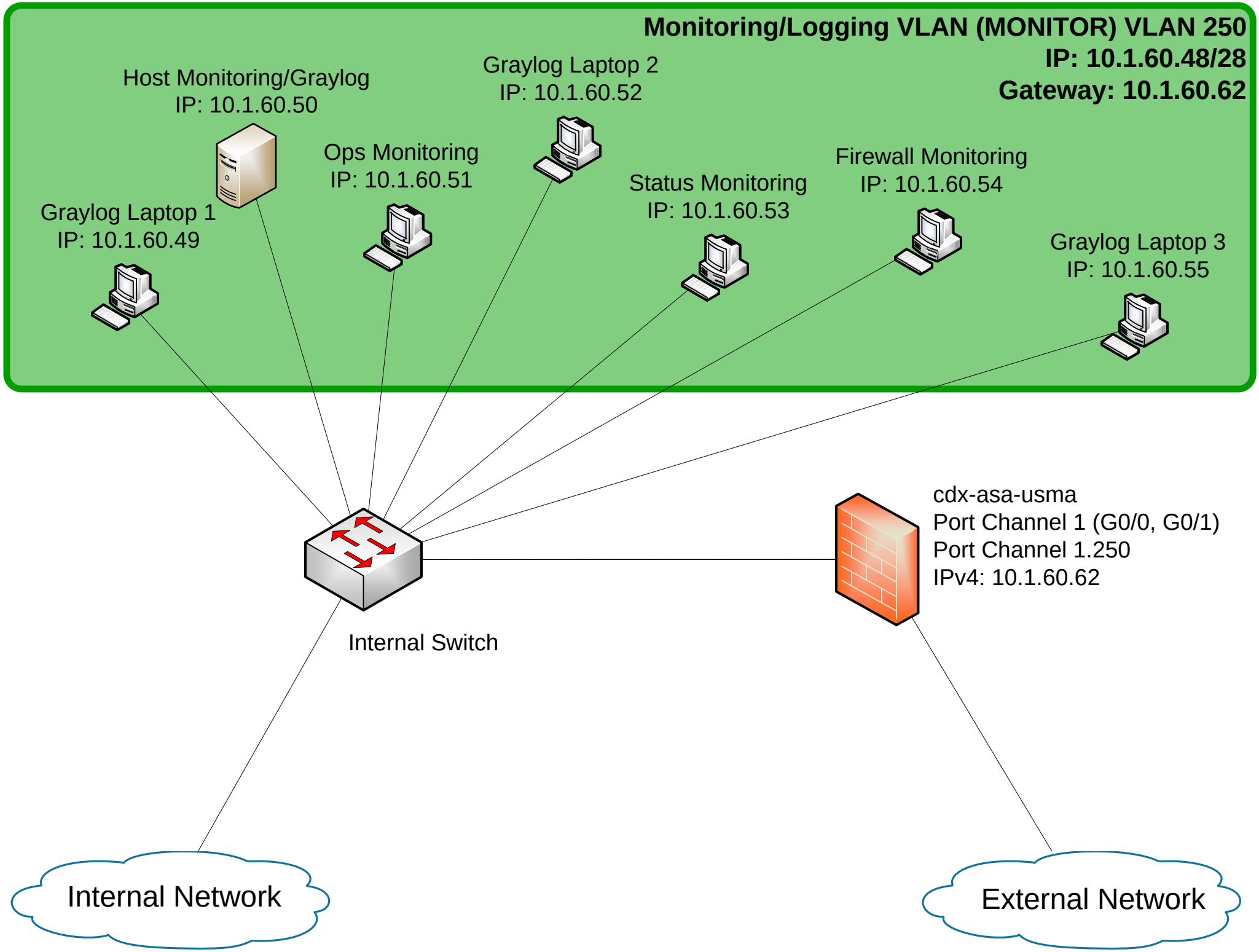
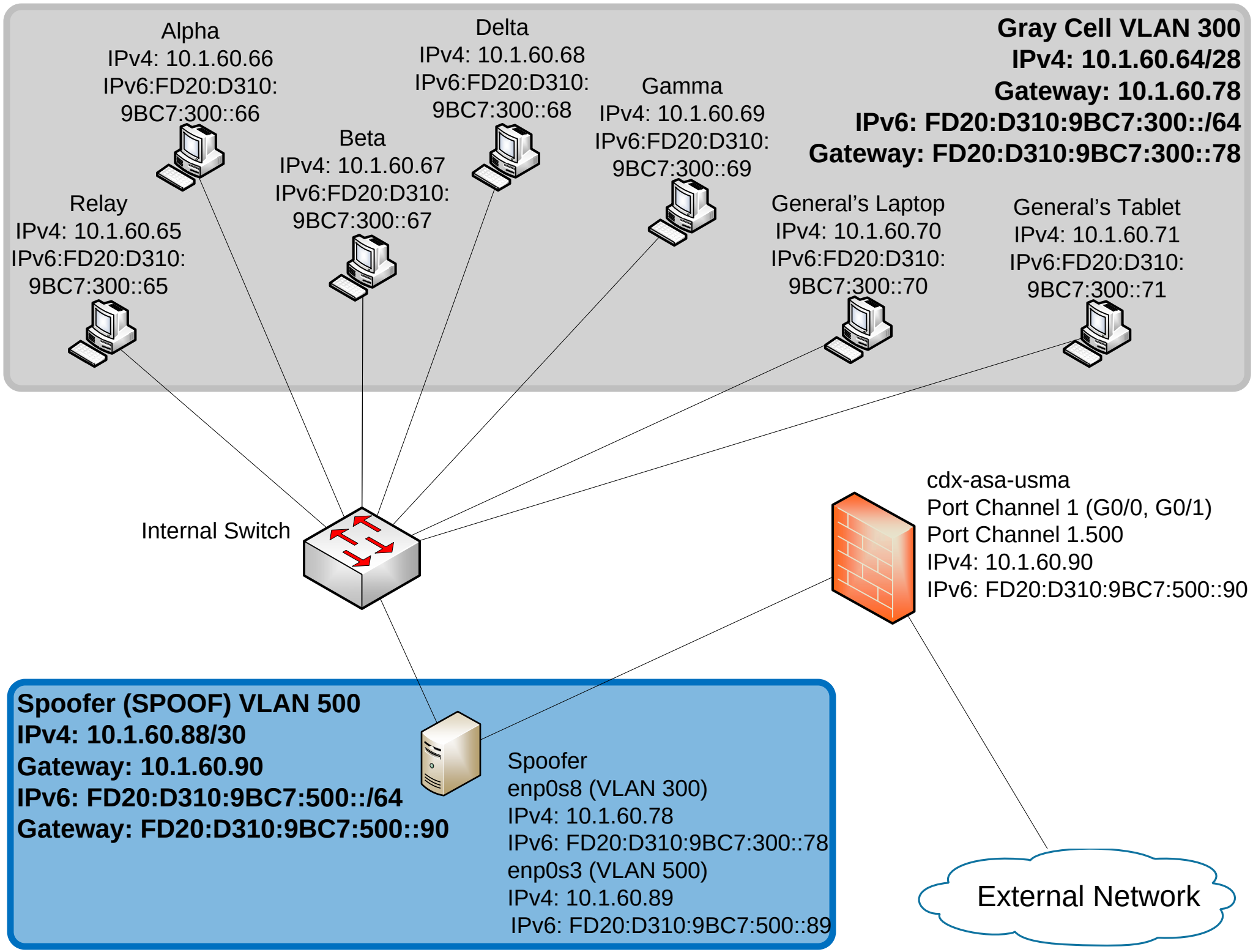
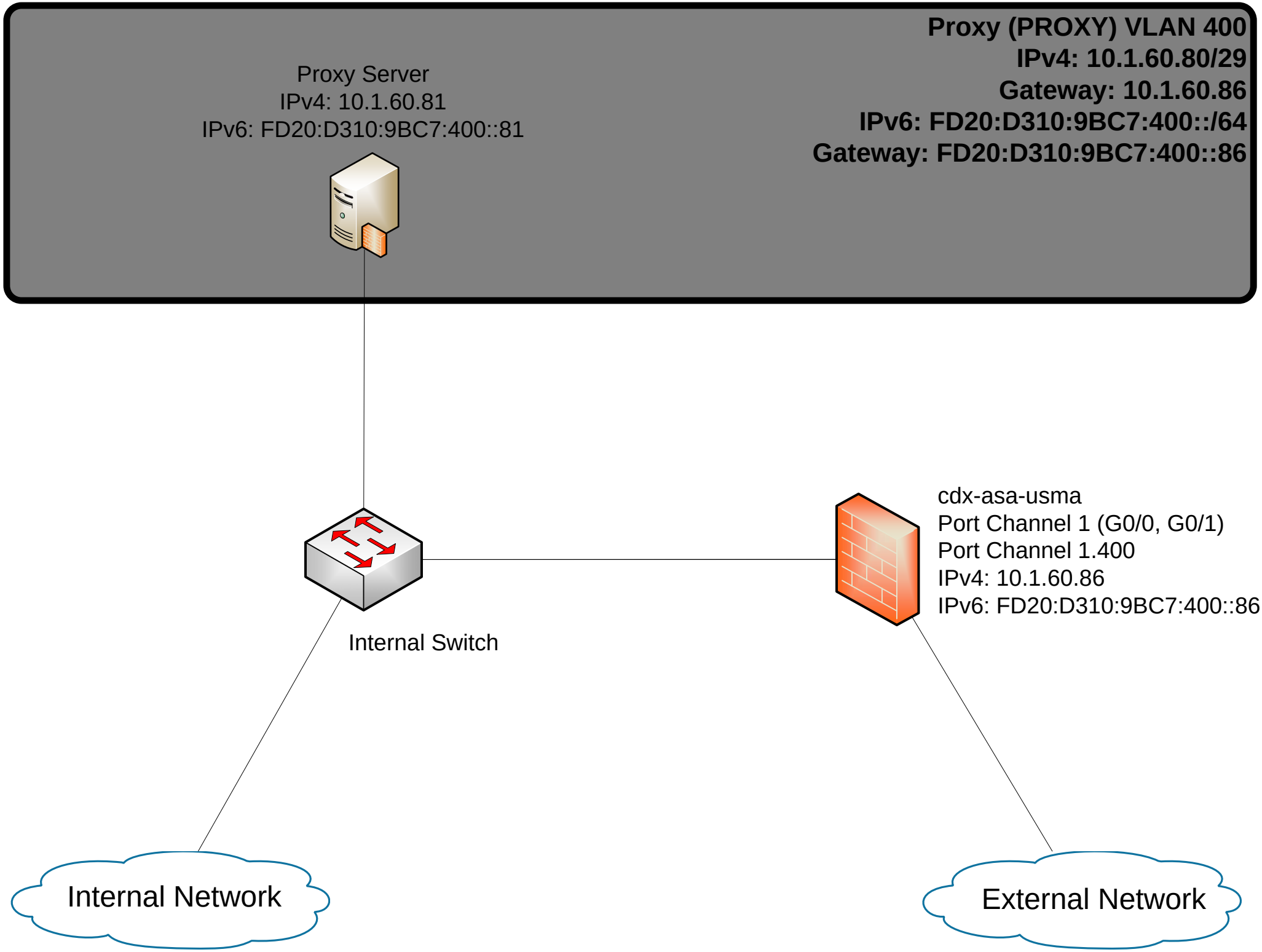

External Services (DMZ)
VLAN 100
Web Server
FTP Server
Web Server Backup
Email Server
DNS Server 1
DNS Server 2
External Network
Firewall
Windows Logger
(WINLOG)
VLAN 700
Windows Event Collector
Gray Cell Web App
(GRAYWEB)
VLAN 600
Web App
Spoofer (SPOOF)
VLAN 500
Spoofer
Gray Cell (GRAY)
VLAN 300
Internal Services (BLUE)
VLAN 200
Active Directory/DNS
Windows Admin
Yum Repo
Internal Switch
Proxy (PROXY)
VLAN 400
Proxy Server
Monitoring/Logging (MONITOR)
VLAN 250
Host Mntr./
graylog
Status Mntr.
Graylog Laptop 2
Firewall Mntr.
Ops Mntr.
Graylog Laptop 1
Graylog Laptop 3
Gray Cell (GRAY)
VLAN 300
Relay
Gamma
Alpha
General's Laptop
Delta
Beta
General's Tablet

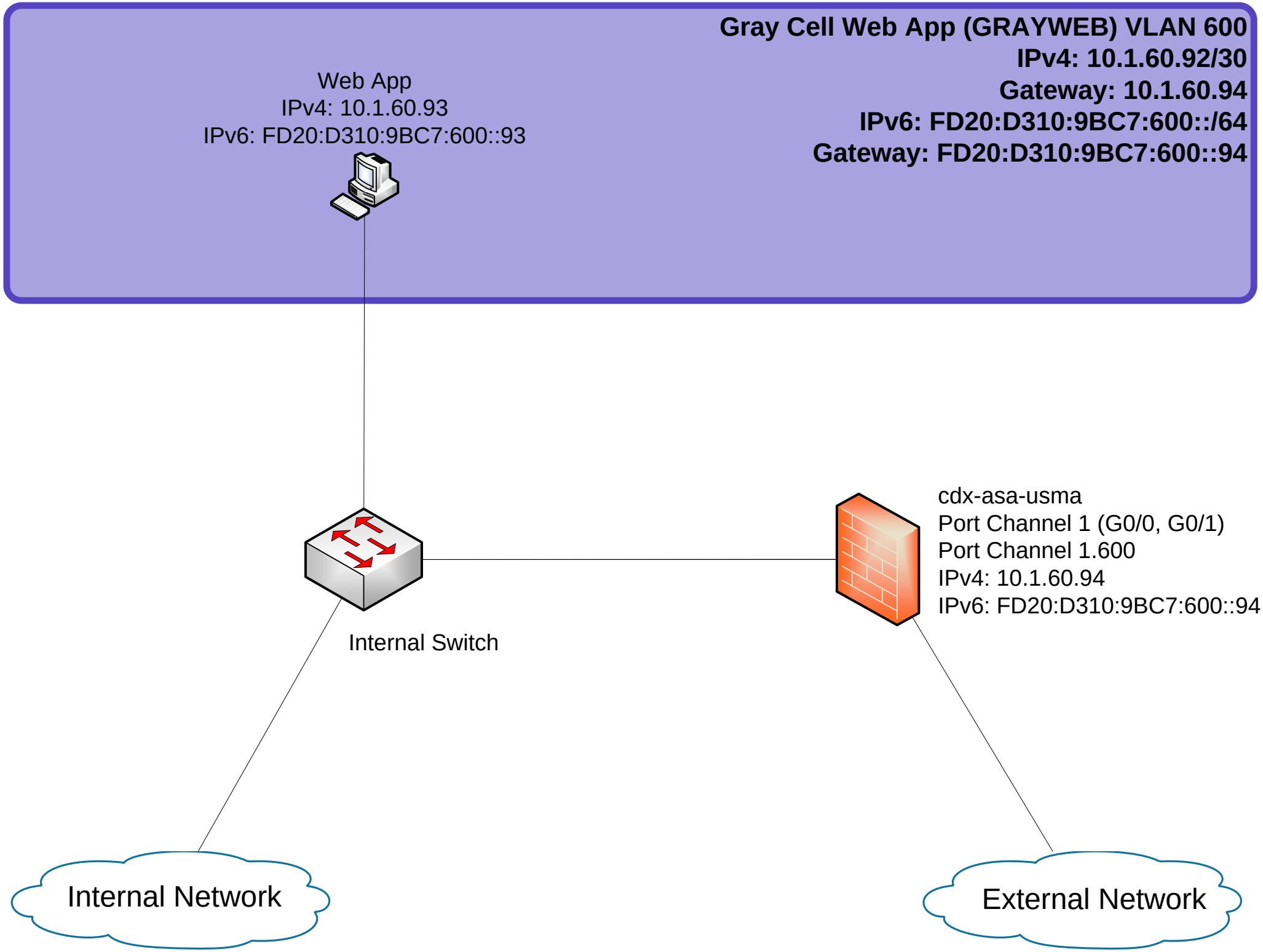

External Services VLAN (DMZ) VLAN 100
IPv4: 10.1.60.0/27
Gateway: 10.1.60.30
IPv6: FD20:D310:9BC7:100::/64
Gateway: FD20:D310:9BC7:100::30
Web Server
IP: 10.1.60.2
IPv6: FD20:D310:9BC7:100::2
Web Server Backup
IP: 10.1.60.3
IPv6: FD20:D310:9BC7:100::3
Email Server
IP: 10.1.60.1
FTP Server
IP: 10.1.60.4
DNS Server 1
IPv4: 10.1.60.5
IPv6: FD20:D310:9BC7:100::5
DNS Server 2
IPv4: 10.1.60.6
IPv6: FD20:D310:9BC7:100::6
Internal Switch
cdx-asa-usma
Port Channel 1 (G0/0, G0/1)
Port Channel 1.100
IPv4: 10.1.60.30
IPv6: FD20:D310:9BC7:100::30
Internal Network
External Network

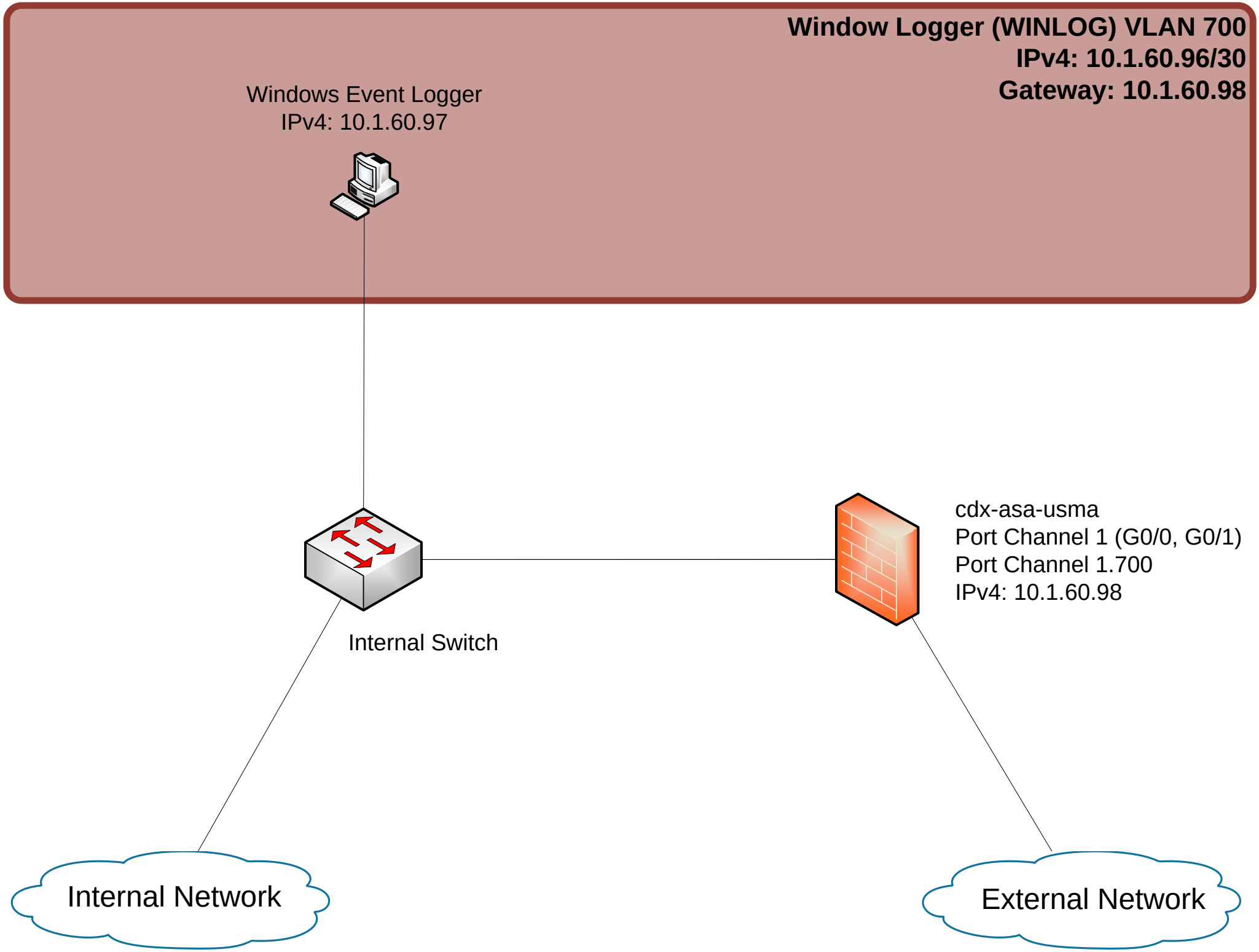

Internal Services (BLUE) VLAN 200
IP: 10.1.60.32/28
Gateway: 10.1.60.46
Active Directory & DNS
IP: 10.1.60.33
Windows Admin
IP: 10.1.60.34
Yum Repo
IP: 10.1.60.35
Internal Switch
cdx-asa-usma
Port Channel 1 (G0/0, G0/1)
Port Channel 1.200
IPv4: 10.1.60.46
Internal Network
External Network

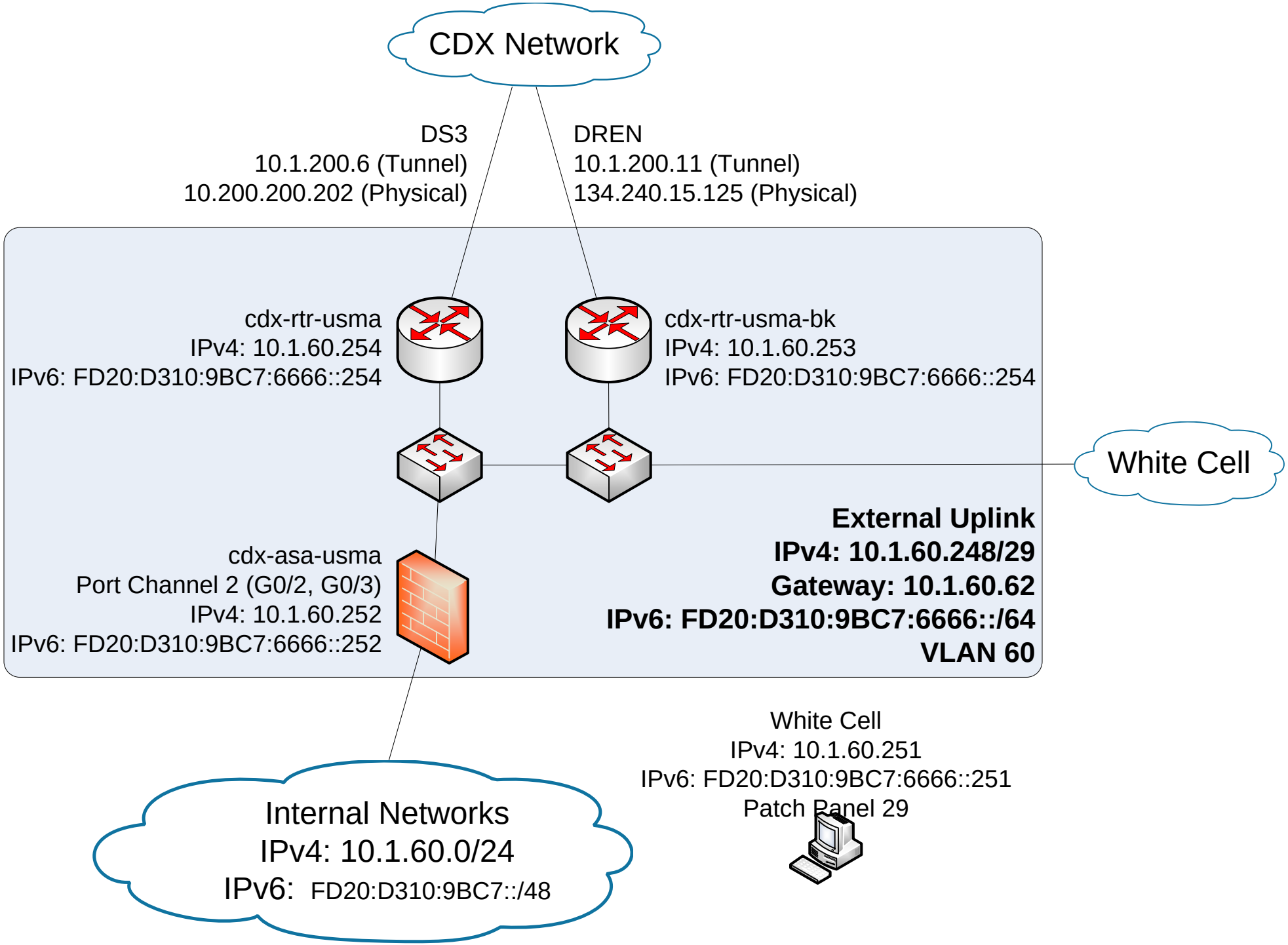

Monitoring/Logging VLAN (MONITOR) VLAN 250
IP: 10.1.60.48/28
Gateway: 10.1.60.62
Host Monitoring/Graylog
IP: 10.1.60.50
Graylog Laptop 2
IP: 10.1.60.52
Ops Monitoring
IP: 10.1.60.51
Graylog Laptop 1
IP: 10.1.60.49
Status Monitoring
IP: 10.1.60.53
Firewall Monitoring
IP: 10.1.60.54
Graylog Laptop 3
IP: 10.1.60.55
Internal Switch
cdx-asa-usma
Port Channel 1 (G0/0, G0/1)
Port Channel 1.250
IPv4: 10.1.60.62
Internal Network
External Network

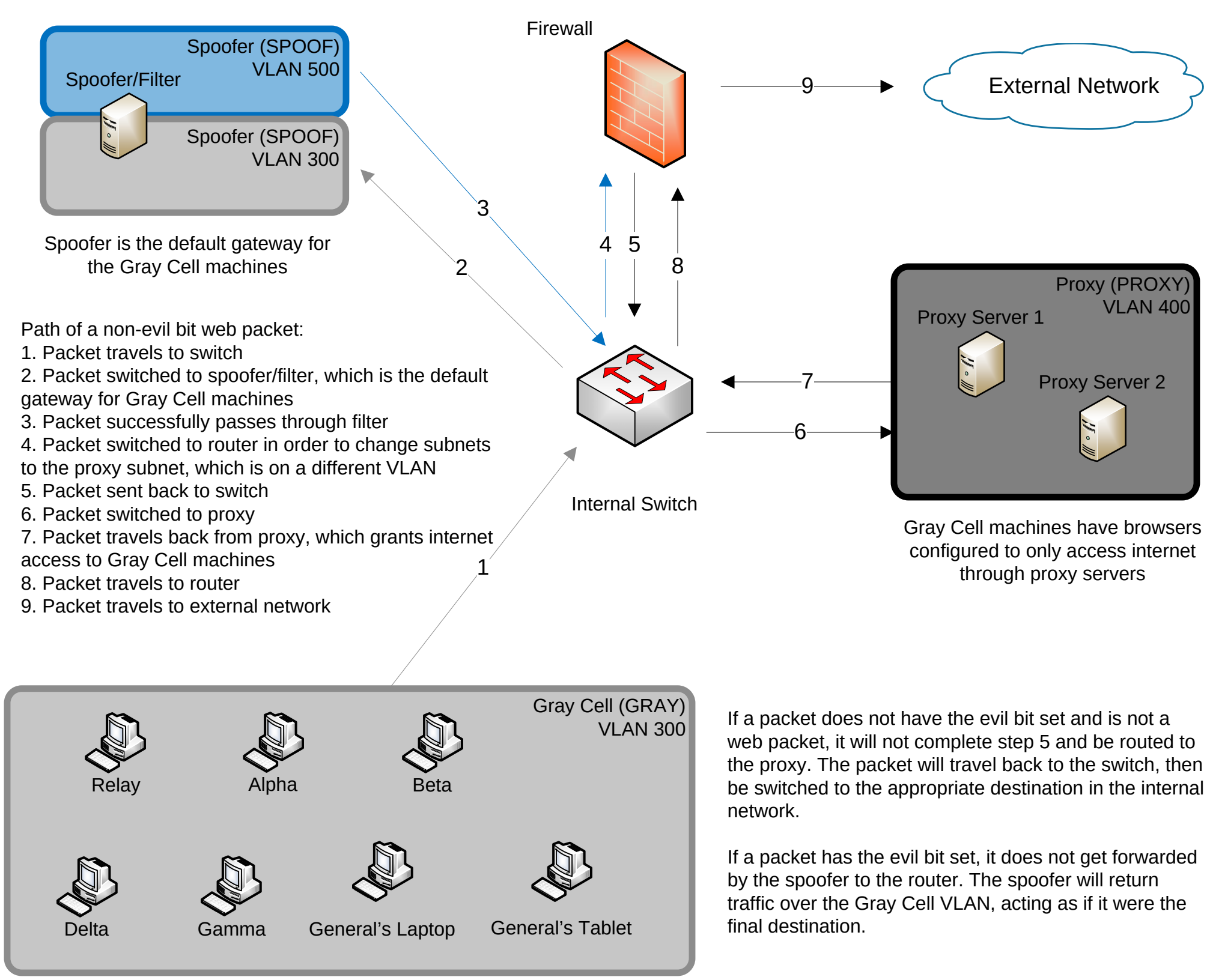

Gray Cell VLAN 300
IPv4: 10.1.60.64/28
Gateway: 10.1.60.78
IPv6: FD20:D310:9BC7:300::/64
Gateway: FD20:D310:9BC7:300::78
Alpha
IPv4: 10.1.60.66
IPv6:FD20:D310:
9BC7:300::66
Beta
IPv4: 10.1.60.67
IPv6:FD20:D310:
9BC7:300::67
Delta
IPv4: 10.1.60.68
IPv6:FD20:D310:
9BC7:300::68
Gamma
IPv4: 10.1.60.69
IPv6:FD20:D310:
9BC7:300::69
Relay
IPv4: 10.1.60.65
IPv6:FD20:D310:
9BC7:300::65
General's Laptop
IPv4: 10.1.60.70
IPv6:FD20:D310:
9BC7:300::70
General's Tablet
IPv4: 10.1.60.71
IPv6:FD20:D310:
9BC7:300::71
Internal Switch
cdx-asa-usma
Port Channel 1 (G0/0, G0/1)
Port Channel 1.500
IPv4: 10.1.60.90
IPv6: FD20:D310:9BC7:500::90
Spoofer (SPOOF) VLAN 500
IPv4: 10.1.60.88/30
Gateway: 10.1.60.90
IPv6: FD20:D310:9BC7:500::/64
Gateway: FD20:D310:9BC7:500::90
Spoofer
enp0s8 (VLAN 300)
IPv4: 10.1.60.78
IPv6: FD20:D310:9BC7:300::78
enp0s3 (VLAN 500)
IPv4: 10.1.60.89
IPv6: FD20:D310:9BC7:500::89
External Network

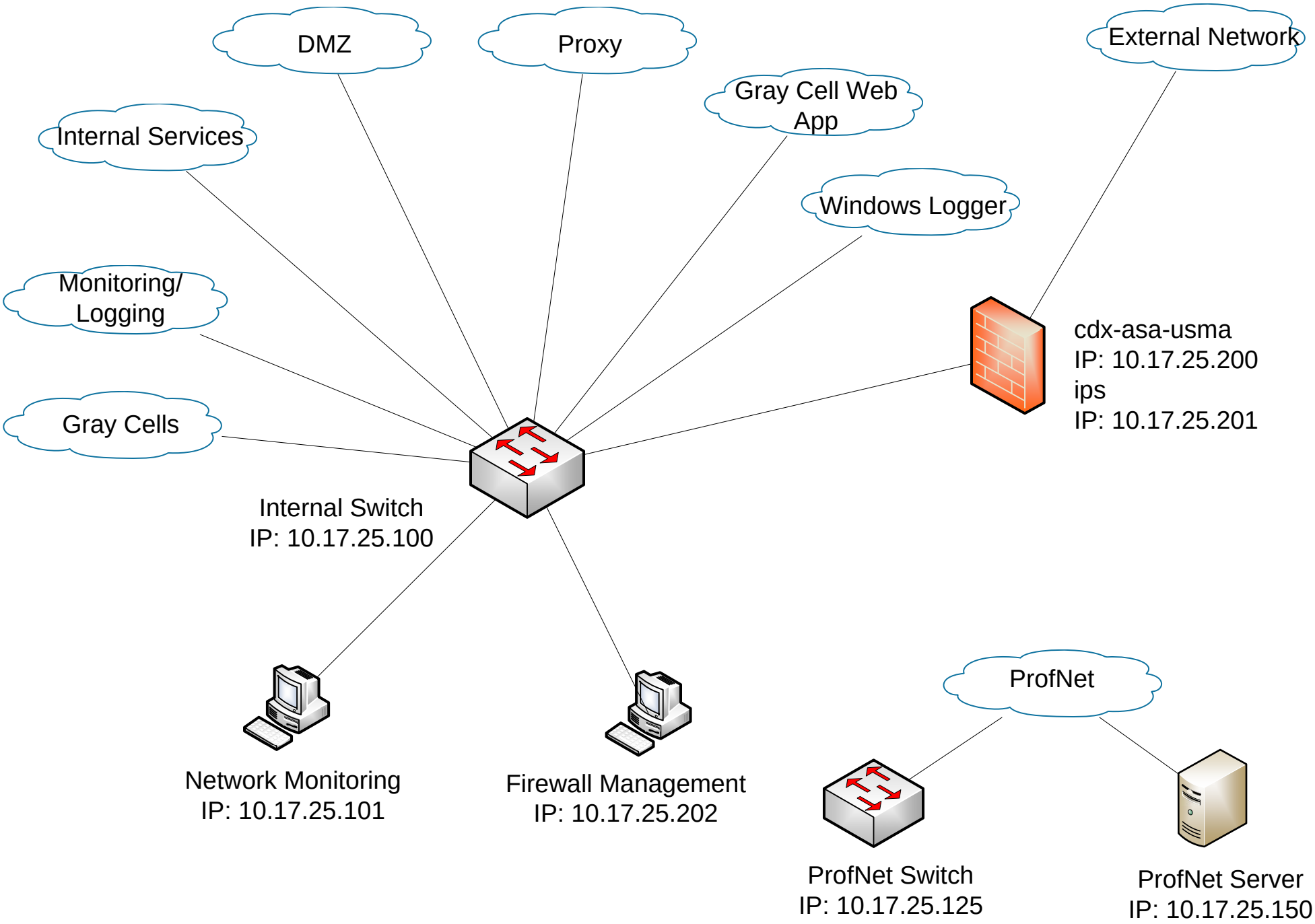

Proxy (PROXY) VLAN 400
IPv4: 10.1.60.80/29
Gateway: 10.1.60.86
IPv6: FD20:D310:9BC7:400::/64
Gateway: FD20:D310:9BC7:400::86
Proxy Server
IPv4: 10.1.60.81
IPv6: FD20:D310:9BC7:400::81
cdx-asa-usma
Port Channel 1 (G0/0, G0/1)
Port Channel 1.400
IPv4: 10.1.60.86
IPv6: FD20:D310:9BC7:400::86
Internal Switch
Internal Network
External Network


Gray Cell Web App (GRAYWEB) VLAN 600
IPv4: 10.1.60.92/30
Gateway: 10.1.60.94
IPv6: FD20:D310:9BC7:600::/64
Gateway: FD20:D310:9BC7:600::94
Web App
IPv4: 10.1.60.93
IPv6: FD20:D310:9BC7:600::93
Internal Switch
cdx-asa-usma
Port Channel 1 (G0/0, G0/1)
Port Channel 1.600
IPv4: 10.1.60.94
IPv6: FD20:D310:9BC7:600::94
Internal Network
External Network


Window Logger (WINLOG) VLAN 700
IPv4: 10.1.60.96/30
Gateway: 10.1.60.98
Windows Event Logger
IPv4: 10.1.60.97
Internal Switch
cdx-asa-usma
Port Channel 1 (G0/0, G0/1)
Port Channel 1.700
IPv4: 10.1.60.98
Internal Network
External Network


CDX Network
DS3
10.1.200.6 (Tunnel)
10.200.200.202 (Physical)
DREN
10.1.200.11 (Tunnel)
134.240.15.125 (Physical)
cdx-rtr-usma
IPv4: 10.1.60.254
IPv6: FD20:D310:9BC7:6666::254
cdx-rtr-usma-bk
IPv4: 10.1.60.253
IPv6: FD20:D310:9BC7:6666::254
White Cell
cdx-asa-usma
Port Channel 2 (G0/2, G0/3)
IPv4: 10.1.60.252
IPv6: FD20:D310:9BC7:6666::252
External Uplink
IPv4: 10.1.60.248/29
Gateway: 10.1.60.62
IPv6: FD20:D310:9BC7:6666::/64
VLAN 60
White Cell
IPv4: 10.1.60.251
IPv6: FD20:D310:9BC7:6666::251
Patch Panel 29
Internal Networks
IPv4: 10.1.60.0/24
IPv6: FD20:D310:9BC7::/48


Spoofer (SPOOF)
VLAN 500
Spoofer/Filter
Spoofer (SPOOF)
VLAN 300
Spoofer is the default gateway for the Gray Cell machines
Firewall
External Network
9
3
2
4
5
8
Proxy (PROXY)
VLAN 400
Proxy Server 1
Proxy Server 2
7
6
Internal Switch
Gray Cell machines have browsers configured to only access internet through proxy servers
Path of a non-evil bit web packet:
1. Packet travels to switch
2. Packet switched to spoofer/filter, which is the default gateway for Gray Cell machines
3. Packet successfully passes through filter
4. Packet switched to router in order to change subnets to the proxy subnet, which is on a different VLAN
5. Packet sent back to switch
6. Packet switched to proxy
7. Packet travels back from proxy, which grants internet access to Gray Cell machines
8. Packet travels to router
9. Packet travels to external network
1
Gray Cell (GRAY)
VLAN 300
Relay
Alpha
Beta
Delta
Gamma
General's Laptop
General's Tablet
If a packet does not have the evil bit set and is not a web packet, it will not complete step 5 and be routed to the proxy. The packet will travel back to the switch, then be switched to the appropriate destination in the internal network.
If a packet has the evil bit set, it does not get forwarded by the spoofer to the router. The spoofer will return traffic over the Gray Cell VLAN, acting as if it were the final destination.


DMZ
Proxy
External Network
Gray Cell Web App
Internal Services
Windows Logger
Monitoring/ Logging
cdx-asa-usma
IP: 10.17.25.200
ips
IP: 10.17.25.201
Gray Cells
Internal Switch
IP: 10.17.25.100
Network Monitoring
IP: 10.17.25.101
Firewall Management
IP: 10.17.25.202
ProfNet
ProfNet Switch
IP: 10.17.25.125
ProfNet Server
IP: 10.17.25.150
Management Network
10.17.25.0/24

Int. Services/BLUE VLAN 200
g0/13: Active Directory/Internal DNS/Windows Admin
g0/14: Yum Repo

Web App VLAN 600
g0/35: Gray Cell Web App
g0/36: Unallocated

Gray Cells VLAN 300
g0/25: Relay
g0/26: Alpha
g0/27: Beta
g0/28: Delta
g0/29: Gamma
g0/30: General's Laptop
g0/31: General's Tablet
g0/32: Unallocated
g0/33: End User Unix
g0/34: Unallocated

Proxy VLAN 400
g0/37: Proxy Server
g0/38: Unallocated
g0/39: Unallocated
g0/40: Unallocated

Services/DMZ VLAN 100
g0/5: Email Server
g0/6: Web Server/Backup/Forum
g0/7: FTP Server
g0/8: DNS Server 1&2
g0/9: Unallocated
g0/10: Unallocated
g0/11: Unallocated
g0/12: Unallocated

Spoofer VLAN 300/500
g0/41: Spoofer Downlink (300)
g0/42: Spoofer Uplink (500)
g0/43: IWAR 3 Monitor
g0/44: Unallocated

Monitoring VLAN 250
g0/15: IWAR 9 Monitor
g0/16: Graylog Laptop 3 (23)
g0/17: Network Monitoring 1
g0/18: Host Monitoring/graylog
g0/19: Ops Monitoring
g0/20: Status Monitoring
g0/21: IWAR 9 Monitor 2
g0/22: IWAR 6 Monitor
g0/23: Graylog Laptop 1 (21)
g0/24: Graylog Laptop 2 (22)

Windows Log VLAN 700
g0/45: Windows Event Logger
g0/46: Unallocated

Packet Captures
g0/1: Official Packet Capture
g0/2: Gray Cell Packet Capture
g0/3: Unallocated
g0/4: Unallocated

Etherchannel
g0/47: Etherchannel 1
g0/48: Etherchannel 2