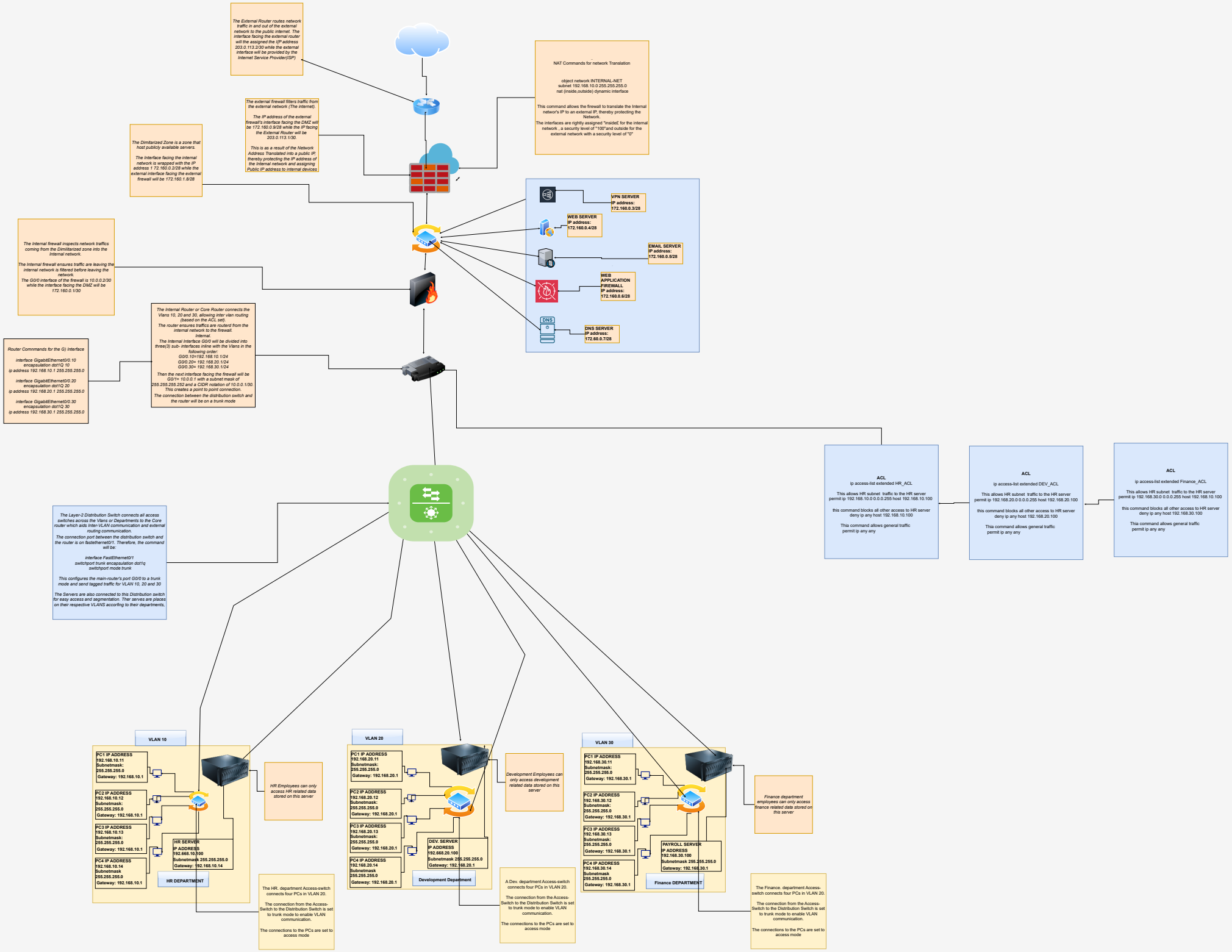
The External Router routes network traffic in and out of the external network to the public internet. The interface facing the external router will the assigned the IP address 203.0.113.2/30 while the external interface will be provided by the Internet Service Provider(ISP)
NAT Commands for network Translation
object network INTERNAL-NET
subnet 192.168.10.0 255.255.255.0
nat (inside,outside) dynamic interface
This command allows the firewall to translate the Internal networ's IP to an external IP, thereby protecting the Network.
The interfaces are rightly assigned "insideE for the internal network , a security level of "100"and outside for the external network with a security level of "0"
The external firewall filters traffic from the external network (The internet).
The IP address of the external firewall's interface facing the DMZ will be 172.160.0.9/28 while the IP facing the External Router will be 203.0.113.1/30.
This is as a result of the Network Address Translated into a public IP, thereby protecting the IP address of the Internal network and assigning Public IP address to internal devices
The Dimitarized Zone is a zone that host publicly available servers.
The Interface facing the internal network is wrapped with the IP address 1 72.160.0.2/28 while the external interface facing the external firewall will be 172.160.1.8/28
VPN SERVER
IP address:
172.160.0.3/28
WEB SERVER
IP address:
172.160.0.4/28
EMAIL SERVER
IP address:
172.160.0.5/28
WEB APPLICATION FIREWALL
IP address:
172.160.0.6/28
DNS
DNS SERVER
IP address:
172.60.0.7/28
The Internal firewall inspects network traffics coming from the Dimilitarized zone into the Internal network.
The Internal firewall ensures traffic are leaving the internal network is filtered before leaving the network.
The G0/0 interface of the firewall is 10.0.0.2/30 while the interface facing the DMZ will be 172.160.0.1/30
Router Commmands for the G) Interface
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
interface GigabitEthernet0/0.30
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.0
The Internal Router or Core Router connects the Vlans 10, 20 and 30, allowing inter vlan routing (based on the ACL set).
The router ensures traffics are routerd from the internal network to the firewall.
Internal.
The Internal Interface G0/0 will be divided into three(3) sub- interfaces inline with the Vlans in the following order:
G0/0.10=192.168.10.1/24
G0/0.20= 192.168.20.1/24
G0/0.30= 192.168.30.1/24
Then the next interface facing the firewall will be G0/1= 10.0.0.1 with a subnet mask of 255.255.255.252 and a CIDR notation of 10.0.0.1/30.
This creates a point to point connection.
The connection between the distribution switch and the router will be on a trunk mode
ACL
ip access-list extended HR_ACL
This allows HR subnet traffic to the HR server
permit ip 192.168.10.0 0.0.0.255 host 192.168.10.100
this command blocks all other access to HR server
deny ip any host 192.168.10.100
Tnis command allows general traffic
permit ip any any
ACL
ip access-list extended DEV_ACL
This allows HR subnet traffic to the HR server
permit ip 192.168.20.0 0.0.0.255 host 192.168.20.100
this command blocks all other access to HR server
deny ip any host 192.168.20.100
Thia command allows general traffic
permit ip any any
ACL
ip access-list extended Finance_ACL
This allows HR subnet traffic to the HR server
permit ip 192.168.30.0 0.0.0.255 host 192.168.10.100
this command blocks all other access to HR server
deny ip any host 192.168.30.100
Thia command allows general traffic
permit ip any any
The Layer-2 Distribution Switch connects all access switches across the Vlans or Departments to the Core router which aids Inter-VLAN communication and external routing communication.
The connection port between the distribution switch and the router is on fastethernet0/1. Therefore, the command will be:
interface FastEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
This configures the main-router's port G0/0 to a trunk mode and send tagged traffic for VLAN 10, 20 and 30
The Servers are also connected to this Distribution switch for easy access and segmentation. Ther serves are places on their respective VLANS accorfing to their departments,
VLAN 10
PC1 IP ADDRESS
192.168.10.11
Subnetmask:
255.255.255.0
Gateway: 192.168.10.1
PC2 IP ADDRESS
192.168.10.12
Subnetmask:
255.255.255.0
Gateway: 192.168.10.1
PC3 IP ADDRESS
192.168.10.13
Subnetmask:
255.255.255.0
Gateway: 192.168.10.1
PC4 IP ADDRESS
192.168.10.14
Subnetmask
255.255.255.0
Gateway: 192.168.10.1
HR SERVER
IP ADDRESS
192.668.10.100
Subnetmask 255.255.255.0
Gateway: 192.168.10.14
HR DEPARTMENT
HR Employees can only access HR related data stored on this server
The HR. department Access-switch connects four PCs in VLAN 20.
The connection from the Access-Switch to the Distribution Switch is set to trunk mode to enable VLAN communication.
The connections to the PCs are set to access mode
VLAN 20
PC1 IP ADDRESS
192.168.20.11
Subnetmask:
255.255.255.0
Gateway: 192.168.20.1
PC2 IP ADDRESS
192.168.20.12
Subnetmask:
255.255.255.0
Gateway: 192.168.20.1
PC3 IP ADDRESS
192.168.20.13
Subnetmask:
255.255.255.0
Gateway: 192.168.20.1
PC4 IP ADDRESS
192.168.20.14
Subnetmask
255.255.255.0
Gateway: 192.168.20.1
DEV. SERVER
IP ADDRESS
192.668.20.100
Subnetmask 255.255.255.0
Gateway: 192.168.20.1
Development Department
Development Employees can only access development related data stored on this server
A Dev. department Access-switch connects four PCs in VLAN 20.
The connection from the Access-Switch to the Distribution Switch is set to trunk mode to enable VLAN communication.
The connections to the PCs are set to access mode
VLAN 30
PC1 IP ADDRESS
192.168.30.11
Subnetmask:
255.255.255.0
Gateway: 192.168.30.1
PC2 IP ADDRESS
192.168.30.12
Subnetmask:
255.255.255.0
Gateway: 192.168.30.1
PC3 IP ADDRESS
192.168.30.13
Subnetmask:
255.255.255.0
Gateway: 192.168.30.1
PC4 IP ADDRESS
192.168.30.14
Subnetmask
255.255.255.0
Gateway: 192.168.30.1
PAYROLL SERVER
IP ADDRESS
192.168.30.100
Subnetmask 255.255.255.0
Gateway: 192.168.30.1
Finance DEPARTMENT
Finance department employees can only access finance related data stored on this server
The Finance. department Access-switch connects four PCs in VLAN 20.
The connection from the Access-Switch to the Distribution Switch is set to trunk mode to enable VLAN communication.
The connections to the PCs are set to access mode