**Network Routing Switching Techniques**

At the moment the network is configured like this:



This is working well at the moment – the routes look a bit like this:



Which is ideal as we don’t want any perspective voice traffic to be encrypted as it loses the DSCP bit for Quality of Service (QOS).

However if we can’t purchase the cisco image that allows us to do this you need to be able to revert to something else.

**Using the Firewall to do the Policy Based Routing as yet untested!:**



Again the routing would look like this:



To make this change the following would need to be done:

1. MPLS routers need to have their 10.x.10.253 interfaces shutdown
2. MPLS routers need to have static routes removed
3. MPLS routers need to have static routes added to point to MPLS interface of Firewall
4. Firewall needs to have Policy Routing configured
5. Firewall needs to have IP spoofing configured to allow traffic
6. Firewall needs to have access rules applied
7. Core switches need to have routing map removed from VLAN interfaces

**Configuration Details:**

**On ES MPLS router:**

Conf t

Int gi0/2

No ip address

Shutdown

Exit

No ip route 172.16.10.0 255.255.255.0 10.10.10.254

Ip route 172.16.10.0 255.255.255.0 192.168.100.1

Ip route 10.10.10.0 255.255.255.0 192.168.100.1

Exit

Copy run start

**On BA MPLS router:**

Conf t

Int gi0/2

No ip address

Shutdown

Exit

No ip route 172.16.40.0 255.255.255.0 10.40.10.254

Ip route 172.16.40.0 255.255.255.0 192.168.200.1

Ip route 10.40.10.0 255.255.255.0 192.168.200.1

Exit

Copy run start

**On ES Firewall:**

**Policy Based Routing Matrix:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Subnet Mask** | **Destination** | **Subnet Mask** | **Next Hop** |
| 10.10.10.0 | 255.255.255.0 | 10.40.10.0 | 255.255.255.0 | 192.168.100.10 |
| 10.10.10.0 | 255.255.255.0 | 172.16.40.0 | 255.255.255.0 | 192.168.100.10 |
| 172.16.10.0 | 255.255.255.0 | 10.40.10.0 | 255.255.255.0 | 192.168.100.10 |
| 10.40.10.0 | 255.255.255.0 | 10.10.10.0 | 255.255.255.0 | 172.16.10.10 |
| 172.16.40.0 | 255.255.255.0 | 10.10.10.0 | 255.255.255.0 | 172.16.10.10 |

**Anti Spoofing:**

Following accepted on 192.168.100.1 and 172.16.10.1

10.10.10.0

172.16.40.0

172.16.10.0

10.40.10.0

**Firewall Rules:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Source | Subnet Mask | Destination | Subnet Mask | Service | Action |
| 10.10.10.0 | 255.255.255.0 | 10.40.10.0 | 255.255.255.0 | Any | Allow |
| 10.10.10.0 | 255.255.255.0 | 172.16.40.0 | 255.255.255.0 | Any | Allow |
| 172.16.10.0 | 255.255.255.0 | 10.40.10.0 | 255.255.255.0 | Any | Allow |
| 10.40.10.0 | 255.255.255.0 | 10.10.10.0 | 255.255.255.0 | Any | Allow |
| 172.16.40.0 | 255.255.255.0 | 10.10.10.0 | 255.255.255.0 | Any | Allow |
| 10.40.10.0 | 255.255.255.0 | 172.16.10.0 | 255.255.255.0 | Any | Allow |

**On BA Firewall:**

**Policy Based Routing Matrix:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Subnet Mask** | **Destination** | **Subnet Mask** | **Next Hop** |
| 10.40.10.0 | 255.255.255.0 | 10.10.10.0 | 255.255.255.0 | 192.168.200.10 |
| 10.40.10.0 | 255.255.255.0 | 172.16.10.0 | 255.255.255.0 | 192.168.200.10 |
| 172.16.40.0 | 255.255.255.0 | 10.10.10.0 | 255.255.255.0 | 192.168.200.10 |
| 10.10.10.0 | 255.255.255.0 | 10.40.10.0 | 255.255.255.0 | 172.16.40.10 |
| 172.16.10.0 | 255.255.255.0 | 10.40.10.0 | 255.255.255.0 | 172.16.40.10 |

**Anti Spoofing:**

Following accepted on 192.168.200.1 and 172.16.40.1

10.10.10.0

172.16.40.0

172.16.10.0

10.40.10.0

**Firewall Rules:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Source | Subnet Mask | Destination | Subnet Mask | Service | Action |
| 10.40.10.0 | 255.255.255.0 | 10.10.10.0 | 255.255.255.0 | Any | Allow |
| 10.40.10.0 | 255.255.255.0 | 172.16.10.0 | 255.255.255.0 | Any | Allow |
| 172.16.40.0 | 255.255.255.0 | 10.10.10.0 | 255.255.255.0 | Any | Allow |
| 10.10.10.0 | 255.255.255.0 | 10.40.10.0 | 255.255.255.0 | Any | Allow |
| 172.16.10.0 | 255.255.255.0 | 10.40.10.0 | 255.255.255.0 | Any | Allow |
| 10.10.10.0 | 255.255.255.0 | 172.16.40.0 | 255.255.255.0 | Any | Allow |

**On ES Core Switch:**

Conf t

Int vlan100

No ip policy route-map VLAN100\_VOIP

Exit

Int vlan10

No ip policy route-map VLAN10\_VOIP

Exit

Exit

Copy run start

Note: this doesn’t get rid of the ACL’s and the policy routes – it just stops them being used on the interfaces – so its pretty quick to reverse the process if you have to.

**On BA Core Switch:**

Conf t

Int vlan100

No ip policy route-map VLAN100\_VOIP

Exit

Int vlan10

No ip policy route-map VLAN10\_VOIP

Exit

exit

Copy run start

Note: this doesn’t get rid of the ACL’s and the policy routes – it just stops them being used on the interfaces – so its pretty quick to reverse the process if you have to.

**Going back to traffic between 10.10.10.0 and 10.40.10.0 going through MPLS but other traffic going through VPN:**



This is how we had it before and leads to some problems – the routes look like this:



What does this mean in reality?

|  |  |  |
| --- | --- | --- |
| **Location** | **Softphone** | **Hardphone** |
| Ealing | Softphones can register and work normally | Hardphones can work normally |
| Bangalore | Softphones can’t register with UK director on LAN | Hardphones can work normally |
| VPN | Softphones can register and work normally | N/A |

To make this change the following would need to be done:

1. Core switches need to have routing map removed from VLAN interfaces
2. Core switches need to have static route for 10.x.10.0 network

**Configuration Details:**

**On ES Core Switch:**

Conf t

Int vlan100

No ip policy-route VLAN100\_VOIP

Exit

Int vlan10

No ip policy-route VLAN10\_VOIP

Exit

Ip route 10.40.10.0 255.255.255.0 10.10.10.253

Exit

Copy run start

**On BA Core Switch:**

Conf t

Int vlan100

No ip policy-route VLAN100\_VOIP

Exit

Int vlan10

No ip policy-route VLAN10\_VOIP

Exit

Ip route 10.10.10.0 255.255.255.0 10.40.10.253

Exit

Copy run start