**Technical Documentation - "Blaze" Enterprise Network**

**1. Introduction and Overview**

This document details the architecture, configuration, and policies of the "Blaze" enterprise network. The network consists of two distinct geographical locations: **CITY 1 BLAZE CENTRAL OFFICE** (Central Office) and **CITY 2 BLAZE SECOND OFFICE** (Second Office).

Connectivity between the offices is provided by a secure IPsec VPN tunnel over the public internet. The internal architecture of each site is based on a hierarchical design, using VLAN segmentation to isolate departmental traffic and increase security and performance.

**Key Implemented Technologies:**

* **Dynamic Routing:** OSPF (Open Shortest Path First) for route exchange within each site and between core devices.
* **Redundancy and High Availability:** HSRP (Hot Standby Router Protocol) for redundant gateways and EtherChannel (LACP) for link aggregation between switches.
* **Security:** Cisco ASA Firewall, Access Control Lists (ACLs), IPsec VPN, DHCP Snooping, Port Security, and secure administrative access via SSH.
* **Network Management:** Centralized logging via Syslog and time synchronization via NTP.

**2. IP Addressing Scheme**

**2.1 Central Office (City 1)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **VLAN Name** | **VLAN ID** | **Subnet** | **Subnet Mask** | **Virtual Gateway (HSRP)** | **Description** |
| **Vlan10-Guest** | **10** | **192.168.1.0** | **255.255.255.224 (/27)** | **192.168.1.1** | Network for guests, with limited Internet access. |
| **Vlan20-Office** | **20** | **192.168.1.32** | **255.255.255.224 (/27)** | **192.168.1.33** | Network for office employees. |
| **Vlan30-IT** | **30** | **192.168.1.64** | **255.255.255.224 (/27)** | **192.168.1.65** | Network for the IT department, with extended privileges. |
| **Vlan40-HR** | **40** | **192.168.1.96** | **255.255.255.224 (/27)** | **192.168.1.97** | Network for the Human Resources department. |
| **Vlan50-Servers** | **50** | **192.168.1.128** | **255.255.255.224 (/27)** | **192.168.1.129** | Dedicated network for central servers. |
| **Vlan60-Managers** | **60** | **192.168.1.160** | **255.255.255.224 (/27)** | **192.168.1.161** | Network for management. |
| **Vlan99-Native** | **99** | - | - | - | Native VLAN for trunk links. |
| **Vlan999-Blackhole** | **999** | - | - | - | VLAN for unused ports (security). |

**2.2. Second Office (City 2)**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **VLAN Name** | | **VLAN ID** | | **Subnet** | | **Subnet Mask** | **Gateway** | | **DHCP Pool** | | |
| **Vlan70-Sales** | | **70** | | **172.16.1.0** | | **255.255.255.224 (/27)** | **172.16.1.1** | | **DHCP\_PoolVlan70** | | |
| **Vlan80-Marketing** | | **80** | | **172.16.1.32** | | **255.255.255.224 (/27)** | **172.16.1.33** | | **DHCP\_PoolVlan80** | | |
| **Vlan99-Native** | **99** | | - | | - | | | - | | Native VLAN for trunk links. |
| **Vlan999-Blackhole** | **999** | | - | | - | | | - | | VLAN for unused ports (security). |

**2.3. Core & WAN Links (Layer 3)**

This table outlines the routed point-to-point connections that form the network backbone and WAN connectivity.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Device** | **Interface 1** | **IP 1** | **Device 2** | **Interface 2** | **IP 2** | **Subnet** | **Description** |
| **MS1** | **Gi0/1** | **10.0.1.1** | **ASA Firewall** | **Gi1/1** | **10.0.1.2** | **10.0.1.0/30** | **Core Link MS1 -> Firewall** |
| **MS2** | **Gi0/2** | **10.0.1.6** | **ASA Firewall** | **Gi1/2** | **10.0.1.5** | **10.0.1.4/30** | **Core Link MS2 -> Firewall** |
| **ASA Firewall** | **Gi1/3** | **10.0.1.9** | **R1-EDGE** | **Gi0/0/1** | **10.0.1.10** | **10.0.1.8/30** | **Link Firewall -> Edge Router** |
| **R1-EDGE** | **Gi0/0/0** | **203.0.113.1** | **R3-ISP** | **Gi0/0/1** | **203.0.113.2** | **203.0.113.0/30** | **WAN Connection City 1** |
| **R2-EDGE** | **Gi0/0/1** | **10.0.2.2** | **MS3** | **Gi0/1** | **10.0.2.1** | **10.0.2.0/30** | **Internal Link City 2** |
| **R2-EDGE** | **Gi0/0/0** | **203.0.113.5** | **R3-ISP** | **Gi0/0/0** | **203.0.113.6** | **203.0.113.4/30** | **WAN Connection City 2** |

**2.4. Internal Switch Links (Layer 2)**

This table details the Layer 2 trunk connections between core, distribution, and access switches.

**City 1 Links :**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Source Device** | **Source Port(s)** | **Destination Device** | **Destination Port(s** | **Link Type** | **Description** |
| **MS1** | **Po1 (Fa0/3, Fa0/4)** | **MS2** | **Po1 (Fa0/3, Fa0/4** | **LACP Port-Channe 1** | **Redundant Trunk between Core Switches** |
| **MS1** | **Fa0/2** | **S1** | **Fa0/2** | **L2 Trunk** | **Uplink from S1 to Core** |
| **MS1** | **Fa0/5** | **S2** | **Fa0/5** | **L2 Trunk** | **Uplink from S2 to Core** |
| **MS1** | **Fa0/6** | **S3** | **Fa0/6** | **L2 Trunk** | **Uplink from S3 to Core** |
| **MS1** | **Fa0/7** | **S4** | **Fa0/7** | **L2 Trunk** | **Uplink from S4 to Core** |
| **MS1** | **Fa0/8** | **S5** | **Fa0/8** | **L2 Trunk** | **Uplink from S5 to Core** |
| **MS1** | **Fa0/1** | **SW** | **Fa0/1** | **L2 Trunk** | **Uplink from SW to Core** |
| **MS2** | **Fa0/5** | **S1** | **Fa0/5** | **L2 Trunk** | **Uplink from S1 to Core** |
| **MS2** | **Fa0/6** | **S2** | **Fa0/6** | **L2 Trunk** | **Uplink from S2 to Core** |
| **MS2** | **Fa0/7** | **S3** | **Fa0/7** | **L2 Trunk** | **Uplink from S3 to Core** |
| **MS2** | **Fa0/8** | **S4** | **Fa0/8** | **L2 Trunk** | **Uplink from S4 to Core** |
| **MS2** | **Fa0/9** | **S5** | **Fa0/9** | **L2 Trunk** | **Uplink from S5 to Core** |
| **MS2** | **Fa0/1** | **SW** | **Fa0/1** | **L2 Trunk** | **Uplink from S6 to Core** |

**City 2 Links:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Source Device** | **Source Port(s)** | **Destination Device** | **Destination Port(s)** | **Link Type** | **Description** |
| **MS3** | **Po1 (Fa0/1, Fa0/2** | **S6** | **Po1 (Fa0/1, Fa0/2)** | **LACP Port-Channel 1** | **Redundant Trunk to Sales Switch** |
| **MS3** | **Po2 (Fa0/3, Fa0/4** | **S7** | **Po2 (Fa0/3, Fa0/4** | **LACP Port-Channel 2** | **Redundant Trunk to Marketing Switch** |

**2.5. OSPF Routing Configuration Details**

This table outlines the specific OSPF configuration for each participating router, including the networks advertised into Area 0.

|  |  |  |  |
| --- | --- | --- | --- |
| Device Name | OSPF Router-ID | Advertised Networks & Key Commands | Notes |
| MS1 | 1.1.1.1 | network 10.0.1.0 0.0.0.3 area 0  network 192.168.1.0 0.0.0.255 area 0  default-information originate | Advertises all City 1 VLANs and the link to the firewall. Injects a default route into the OSPF domain for other devices. |
| MS2 | 2.2.2.2 | network 10.0.1.4 0.0.0.3 area 0  network 192.168.1.0 0.0.0.255 area 0 | Advertises all City 1 VLANs and the redundant link to the firewall. |
| ciscoasa | 3.3.3.3 | network 10.0.1.0 255.255.255.252 area 0  network 10.0.1.4 255.255.255.252 area 0  network 10.0.1.8 255.255.255.252 area 0  redistribute static subnets  redistribute connected subnets | Central OSPF router. Advertises its connected links and redistributes static routes (including the default route) into OSPF. |
| R1-EDGE | 4.4.4.4 | network 10.0.1.8 0.0.0.3 area 0 | Advertises the internal link towards the ASA firewall. |
| R2-EDGE | 6.6.6.6 | network 10.0.2.0 0.0.0.3 area 0  default-information originate | Advertises the internal link towards MS3 and injects a default route for the City 2 site. |
| MS3 | 7.7.7.7 | network 10.0.2.0 0.0.0.3 area 0  network 172.16.1.0 0.0.0.31 area 0  network 172.16.1.32 0.0.0.31 area 0 | Advertises the link to R2-EDGE and the local VLANs for Sales and Marketing. |

**3. Central Office (City 1) Architecture**

**3.1. Core/Distribution Layer (MS1 & MS2)**

The L3 switches MS1 and MS2 (model 3560-24PS) form the network core. They are responsible for inter-VLAN routing and ensure high availability.

* Inter-VLAN Routing: Each switch has SVI (Switch Virtual Interface) interfaces defined for each VLAN, allowing communication between departments.
* **High Availability (HSRP):**
  + HSRP is configured on all VLAN interfaces to provide a redundant gateway.
  + MS1 is configured as the Active router (HSRP priority 110).
  + MS2 is configured as the Standby router (HSRP priority 90).
  + preempt is enabled, ensuring that MS1 automatically becomes active again if it comes back online.
* **Redundancy (EtherChannel):**
  + Interfaces FastEthernet0/3 and FastEthernet0/4 on both switches are aggregated into Port-channel1 using the LACP protocol (mode active). This doubles the bandwidth and provides a redundant path between the two core switches.
* **Routing (OSPF):**
  + Both switches participate in the OSPF process (ID 1, area 0), advertising their directly connected VLAN networks.
  + MS1 has a router-id of 1.1.1.1, and MS2 has a router-id of 2.2.2.2.
  + MS1 distributes a default route (default-information originate) into OSPF, which it receives from the Firewall.
* **Spanning Tree Protocol (STP):**
  + Rapid-PVST is used for fast convergence.
  + MS1 is configured as the primary root bridge for VLANs 10-60 (priority 4096).
  + MS2 is the secondary root bridge (priority 8192).

**3.2. Perimeter Security Layer (ASA Firewall)**

The ciscoasa firewall (ASA Version 9.6) is the central security control point.

* **Security Zones (Interfaces**):
  + inside1 (security-level 100): Connected to MS1. Traffic is permitted by default.
  + inside2 (security-level 50): Connected to MS2. It has a lower trust level.
  + outside (security-level 0): Connected to R1-EDGE. All traffic initiated from this zone is denied by default.
* **Routing (OSPF & Static):**
  + Participates in OSPF (router-id 3.3.3.3) to learn internal routes from MS1/MS2 and to advertise static routes.
  + Has a static default route (0.0.0.0/0) towards R1-EDGE (10.0.1.10) for Internet access.
  + Redistributes static and connected routes into OSPF to provide visibility to the internal network.
* **Access Policies (ACLs):**
  + OUTSIDE-IN: Applied on the outside interface, it allows ICMP and specific traffic (DNS, HTTP/S) to internal servers.
  + INSIDE-IN / INSIDE-IN2: Permit traffic from internal networks to the outside.

**3.3. Edge Layer (R1-EDGE**)

The R1-EDGE router serves as the gateway to the Internet and the termination point for the VPN tunnel.

* **NAT (Network Address Translation):**
  + Configures PAT (Port Address Translation) to allow internal users (network 192.168.1.0/24) to access the Internet using the public IP address of the GigabitEthernet0/0/0 interface.
  + The NAT-R1 ACL excludes traffic destined for the City 2 network (VPN) from being translated.
  + Static NAT publishes the HTTP server (192.168.1.134) on ports 80 and 443.
* **IPsec Site-to-Site VPN:**
  + A crypto map (VPN-MAP) is applied to the outside interface (GigabitEthernet0/0/0).
  + The tunnel is configured with the peer 203.0.113.5 (the public IP of R2-EDGE).
  + The VPN-TRAFFIC ACL defines the traffic to be encrypted: communication between City 1 (192.168.1.0/24) and City 2 (172.16.1.0/24) networks.

**3.4. Access Layer (S1-S5, SW)**

The access layer switches (model 2960-24TT) connect end devices (PCs, printers, IP phones, Access Points).

* Port-Level Security:
  + Port Security: Limits the number of MAC addresses allowed on a port and prevents unauthorized access. mac-address sticky is used to dynamically learn MAC addresses.
  + DHCP Snooping: Prevents rogue DHCP server attacks. Ports to the distribution switches (MS1, MS2) are configured as trust.
  + PortFast & BPDU Guard: Ensures access ports enter the forwarding state immediately and disables them if they receive BPDUs, preventing network loops from unauthorized switch connections.
* Global Security Policies:
  + All unused ports are shut down and assigned to the 999 (blackhole) VLAN.
  + Administrative access (VTY) is allowed only via SSH and is restricted to the IT VLAN (SSH\_ONLY\_VLAN30).

**3.5. Central Services**

Servers are located in VLAN 50.

* DNS/DHCP Server: 192.168.1.133
* HTTP Server ([www.blaze.be](https://www.google.com/url?sa=E&q=http%3A%2F%2Fwww.blaze.be)): 192.168.1.134
* EMAIL Server: 192.168.1.135
* FILE Server: 192.168.1.136
* SYSLOG Server: 192.168.1.137 (all devices are configured to send logs to this server).

4. Second Office (City 2) Architecture

**4.1. Edge Layer (R2-EDGE)**

Similar to R1-EDGE, this router manages the Internet connection and the VPN tunnel.

* NAT/PAT: Configures PAT for the local networks (172.16.1.0/27 and 172.16.1.32/27) using the NAT-R2 ACL, which excludes VPN traffic.
* IPsec VPN: Configures the secondary end of the VPN tunnel, peering with 203.0.113.1 (the public IP of R1-EDGE).
* Routing (OSPF): Distributes a default route to MS3.

**4.2. Distribution/Access Layer (MS3)**

The L3 switch MS3 is the central device of this office, combining distribution and access roles.

* Routing and Gateway: Acts as the gateway for VLAN 70 (Sales) and VLAN 80 (Marketing).
* DHCP Service:
  + MS3 is configured as a DHCP server for both VLANs.
  + It provides IP addresses, the default gateway, and the DNS server (located in City 1 - 192.168.1.133).
* Routing (OSPF): Participates in OSPF (router-id 7.7.7.7) to exchange routes with R2-EDGE and, implicitly, with the Central Office through the VPN tunnel.
* Redundancy (EtherChannel): Uses port-channels to connect redundantly to access switches S6 and S7.

**4.3. Access Layer (S6 & S7)**

These switches connect users from the Sales and Marketing departments and implement the same port-level security policies as the switches in City 1 (Port Security, PortFast, BPDU Guard).

5. External Connectivity (R3-ISP Router)

The R3-ISP router simulates the Internet Service Provider's network. It provides the underlying connectivity fabric that links the two Blaze office sites across the public domain. It is important to note that this device is outside the Blaze enterprise management domain.

**Key Responsibilities & Configuration:**

* Packet Forwarding: Its primary function is to route packets between the public-facing interfaces of the Blaze edge routers: R1-EDGE (203.0.113.1) and R2-EDGE (203.0.113.5).
* Static Routing: The R3-ISP router does not participate in the Blaze OSPF domain. Instead, it uses static routes to direct traffic destined for the internal subnets of City 1 and City 2 back to the correct edge router. For example, any traffic destined for the 192.168.1.0/24 range is forwarded to R1-EDGE's public IP. This configuration simulates how a real ISP would route traffic to a customer's allocated IP block.
* Blackhole Route: The configuration includes the command ip route 0.0.0.0 0.0.0.0 Null0. This is a standard ISP practice. It acts as a blackhole for any traffic that does not match a more specific route in its table, preventing potential routing loops and dropping traffic to unallocated addresses within the ISP's network.

**6. Conclusions and Recommendations**

The "Blaze" network is robustly designed with a strong emphasis on security, redundancy, and segmentation. The configurations demonstrate the application of industry best practices.

Strengths:

* The use of HSRP and EtherChannel ensures high availability.
* Granular segmentation through VLANs effectively isolates broadcast and security domains.
* Port-level security policies (Port Security, DHCP Snooping) harden the network against internal threats.
* Centralized management (Syslog, NTP) and secure access (SSH) simplify administration.

7. Passwords

Enable secret password: cisco

Line console 0 password: cisco

Ssh :

-username: admin

-password: cisco

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |