Security Design Report

Prepared For

Joe’s Snacks Company

To: Mr. Joseph Jasper, CEO, Joe’s Snacks Company

From: Corinne Otten, Network Security Analyst

Date: June 8, 2023

Table of Contents

I. Overview

A. Background

To provide you with a brief background, I have been providing services as a Network Security Analyst for one year. While pursuing my Master of Science in Cybersecurity, Computer Science from DePaul University, I gained much experience in designing and creating network designs for homes, small business, and large enterprises. That experience, combined with my sixteen years of previous legal experience, makes me uniquely qualified to design a customized network that is not only efficient but also complies with today's security legal requirements. I have analyzed the network needs of Joe's Snacks Company, as expressed by Mr. Joseph Jasper, and have prepared a proposal that not only considers the needs for today but also provides options for future growth.

B. Network Requirements and Security Challenges

Joe's Snacks Company (JS) is an e-commerce retailer of snack foods. These goods are sold in two ways: (a) through an e-commerce server – JS-Sales-Server – which is accessible to all Internet users via HTTPS, and (b) through sales employees who take orders over the phone. It is my understanding that there are six servers on the JS network: four that accept requests from clients and send back responses, and two that are application proxies that act as intermediaries between a client and server – receiving responses from the servers, inspecting them, and passing them back to clients.

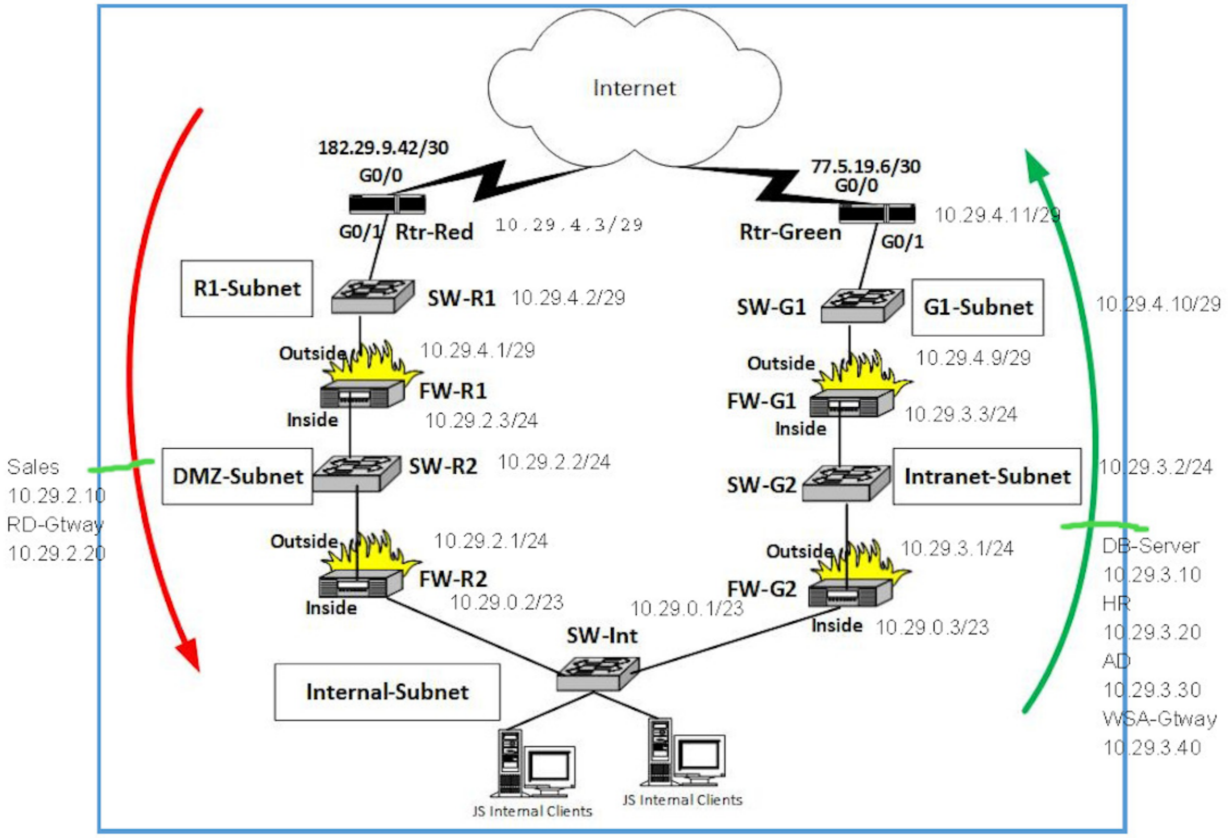
In preparing this design proposal, I have considered several security challenges. First, the design must contain a DMZ-Subnet so that the servers accessible by the public cannot be used as a gateway into the private Internal-Subnet that contains company secrets and confidential data. The same can be said for the private Intranet servers, which should also have a separate subnet. Second, one must expect hackers to threaten the network from without and within and design the network not only for traffic purposes but also for security purposes. The routers and firewalls presented in this design have the following built-in security features: Access Control Lists (ACLs) to filter traffic based on specific criteria; stateful inspection of packets; Virtual Private Network (VPN) support; integrated Intrusion Prevention Systems (IPSs) that detect and prevent a variety of network attacks; Network and Port Address Translation (NAT/PAT) to hide internal IP addresses from external networks; URL filtering; application inspection; and Zone-Based Policy settings. These features have all been considered and will be discussed in this design proposal.

II. Network Architecture

A. Proposed Topology

A dual-path dual-layer network architecture design is the best network design for Joe's Snacks Company. Using this design, two parallel paths are created with dual layers. This allows segregation of traffic per application or traffic type. In this design, the left path with a "Red Rail" is for inbound-initiated traffic originating from outside the internal network and the right path with a "Green Rail" is for outbound-initiated traffic originating from inside the internal network. Additionally, there are two firewalls on each path that provide additional security and redundancy. Other advantages include the ability to: quickly redirect to another path/IP if there is an attack, use two ISPs for that higher redundancy, and simpler firewall configuration. Some disadvantages include increased additional cost and configuration complexity.

Please see the figure below for a representation of this topology.



The JS Network Diagram

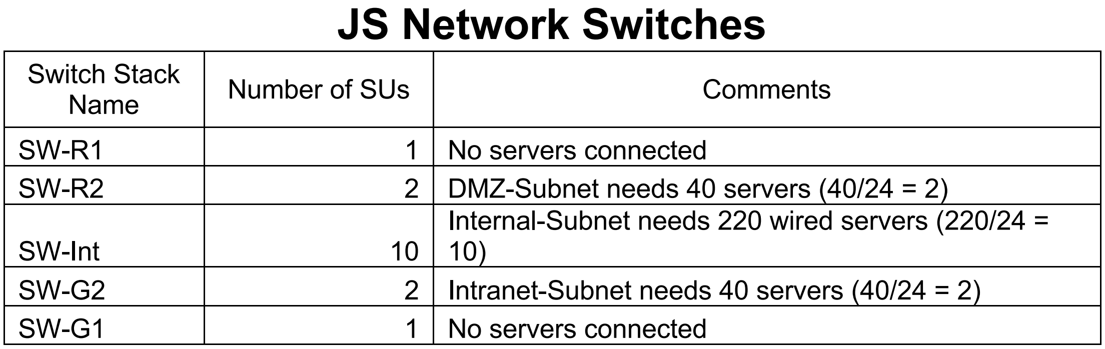
B. Comparison of Alternatives

While a dual-path dual-layer architecture may be more complex and costly to implement than simpler architectures such as a single-path dual-layer or single 2-leg or 3-leg firewall architecture, the benefits make it a worthwhile investment. For instance, the one path in a single-path dual-layer architecture does not allow for the redundancy of a dual-path architecture in which case one path could fail and the other can continue to handle traffic ensuring continuous high-availability. Similarly, two paths allow traffic to be distributed across both paths enabling better load balancing and preventing any single device or path from becoming a bottleneck. Also, different types of applications and traffic can be handled by different paths, so this improves security and makes it easier to manage and troubleshoot the network. Additionally, as the network grows additional devices can be added to each path making it easy to scale the network to meet potential future growth. Finally, in comparison to a 2-leg or 3-leg architecture, the two layers of firewalls increase security; an attacker would need to breach both firewalls to gain access to the Internal Network.

C. Hardware Details

Each of the five switches is a switch stack containing a number of Switch Units (SUs), where each SU is a 24-port switch module, and each port is a 1Gbps Ethernet port. Each switch requires one IP address on its VLAN1 switch virtual interface for management. To determine the number of SUs for each switch, I considered the discussed number of servers that would be connected to each subnet and divided that number by 24 since each server will be connected to and need one port.

Please see the figure below for this calculation.



JS Network Switches

Switch Stack Name	Number of SUs	Comments
SW-R1	1	No servers connected
SW-R2	2	DMZ-Subnet needs 40 servers (40/24 = 2)
SW-Int	10	Internal-Subnet needs 220 wired servers (220/24 = 10)
SW-G2	2	Intranet-Subnet needs 40 servers (40/24 = 2)
SW-G1	1	No servers connected

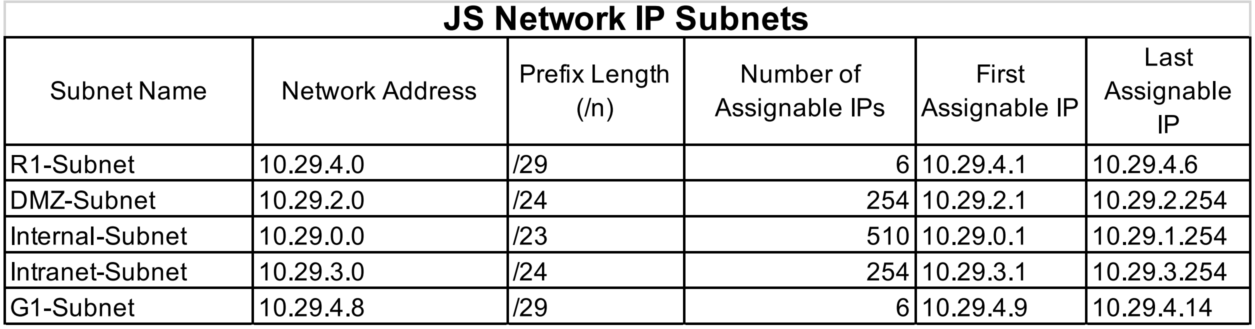
III. IP Addressing

A. Subnets

Based on the network requirement provided to me, I determined a Subnet ID for each of the five subnets in the JS Network. Considering the provided requirements for IP addresses, servers/devices, and subnets, I divided the 10.29.0.0/16 subnet into five smaller subnets. Each subnet must be able to assign a unique IP address to each of its allotted number of devices, and leave some room for growth:

1) R1-Subnet → at least 3 IP addresses needed – starting with 10.29.0.0/16 = prefix length /29 provides 6 assignable IPs
2) DMZ-Subnet → at least 40 IP addresses needed = prefix length /24 provides 254 assignable IPs (leaving room to grow, and /24 is a typical prefix length for company networks)
3) Internal-Subnet → at least 320 IP addresses needed = prefix length /23 provides 510 assignable IPs
4) Intranet-Subnet → at least 40 IP addresses needed = prefix length /24 provides 254 assignable IPs (leaving room to grow, and /24 is a typical prefix length for company networks)
5) G1-Subnet → at least 3 IP addresses needed = prefix length /29 provides 6 assignable IPs

Please see the figure below for more specific IP Subnet information.



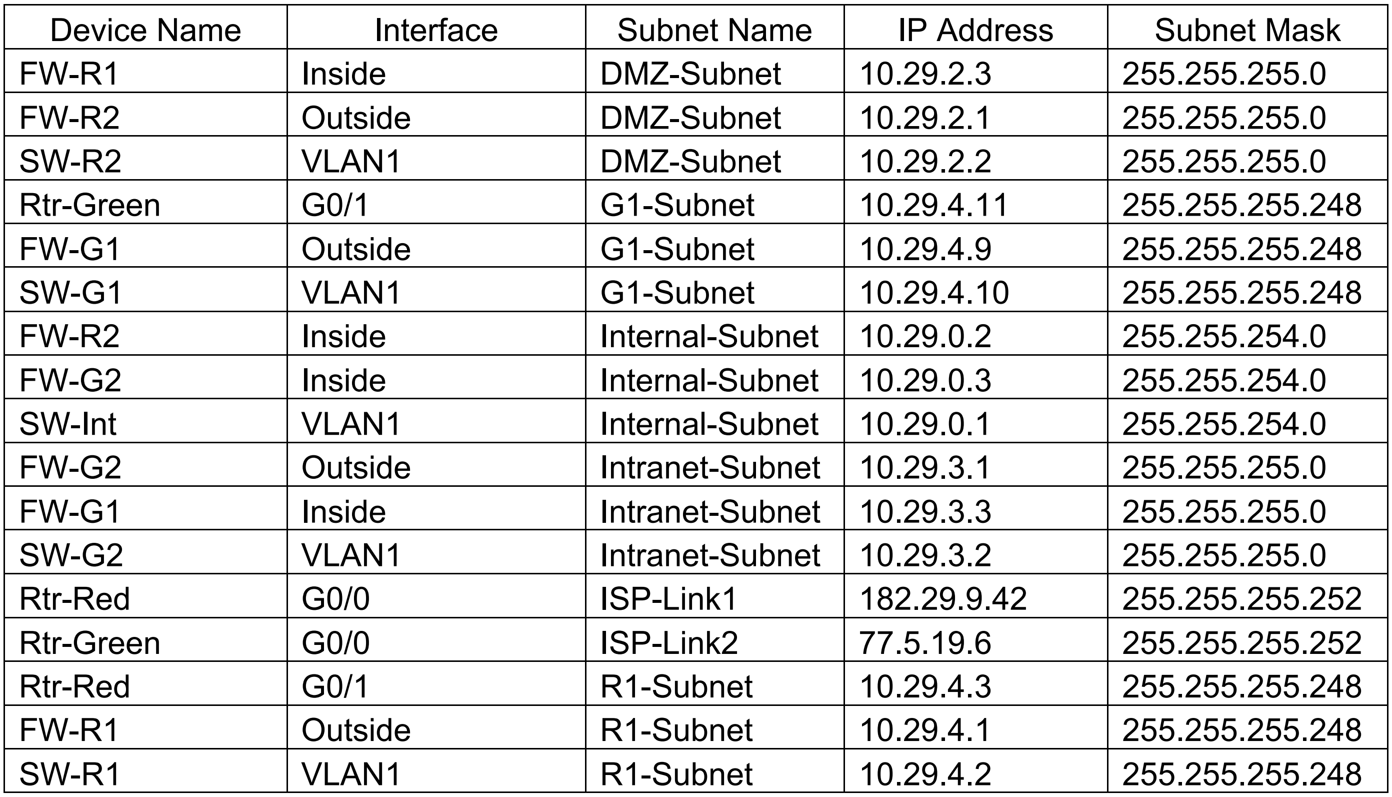
JS Network IP Subnets

Subnet Name	Network Address	Prefix Length (/n)	Number of Assignable IPs	First Assignable IP	Last Assignable IP
R1-Subnet	10.29.4.0	/29	6	10.29.4.1	10.29.4.6
DMZ-Subnet	10.29.2.0	/24	254	10.29.2.1	10.29.2.254
Internal-Subnet	10.29.0.0	/23	510	10.29.0.1	10.29.1.254
Intranet-Subnet	10.29.3.0	/24	254	10.29.3.1	10.29.3.254
G1-Subnet	10.29.4.8	/29	6	10.29.4.9	10.29.4.14

B. Interfaces

With the Subnet IDs decided, I chose specific IP addresses out of those ranges for each device interface in the JS Network. Please see the figure below for details.

JS Network Device Interface IPs



Device Name	Interface	Subnet Name	IP Address	Subnet Mask
FW-R1	Inside	DMZ-Subnet	10.29.2.3	255.255.255.0
FW-R2	Outside	DMZ-Subnet	10.29.2.1	255.255.255.0
SW-R2	VLAN1	DMZ-Subnet	10.29.2.2	255.255.255.0
Rtr-Green	G0/1	G1-Subnet	10.29.4.11	255.255.255.248
FW-G1	Outside	G1-Subnet	10.29.4.9	255.255.255.248
SW-G1	VLAN1	G1-Subnet	10.29.4.10	255.255.255.248
FW-R2	Inside	Internal-Subnet	10.29.0.2	255.255.254.0
FW-G2	Inside	Internal-Subnet	10.29.0.3	255.255.254.0
SW-Int	VLAN1	Internal-Subnet	10.29.0.1	255.255.254.0
FW-G2	Outside	Intranet-Subnet	10.29.3.1	255.255.255.0
FW-G1	Inside	Intranet-Subnet	10.29.3.3	255.255.255.0
SW-G2	VLAN1	Intranet-Subnet	10.29.3.2	255.255.255.0
Rtr-Red	G0/0	ISP-Link1	182.29.9.42	255.255.255.252
Rtr-Green	G0/0	ISP-Link2	77.5.19.6	255.255.255.252
Rtr-Red	G0/1	R1-Subnet	10.29.4.3	255.255.255.248
FW-R1	Outside	R1-Subnet	10.29.4.1	255.255.255.248
SW-R1	VLAN1	R1-Subnet	10.29.4.2	255.255.255.248

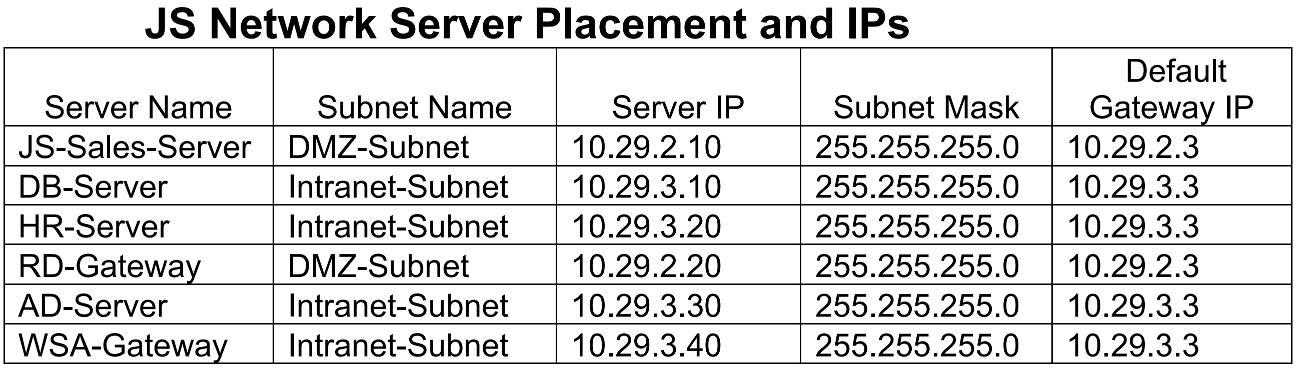
IV. Server Placement and Addressing

I have determined the placement of each server on the JS Network based on the server requirements, Red/Green connection direction requirements, number and function of the six servers, and restriction that servers can only be placed on the DMZ-Subnet or Intranet-Subnet. I placed the following servers as follows:

1) JS-Sales-Server: E-Commerce server for company sales. Internet users connect to this server via HTTPS to place orders. → Because this needs to be accessed by Internet users, this is placed in the DMZ-Subnet.
2) DB-Server: A PostgreSQL server that stores completed snack orders that will be processed and shipped. → Because this contains private data, this is placed in the Intranet-Subnet.
3) HR-Server: An internal Human Resources server. JS employees connect to this server via HTTPS to manage their employment data and employee benefits. → Because this contains private and extremely confidential data, this is placed in the Intranet-Subnet.
4) RD-Gateway: A Microsoft Remote Desktop Gateway that allows authorized remote JS employees out on the public Internet to connect to their workstations via Remote Desktop. → Because this needs to be accessed from the public Internet, this is placed in the DMZ-Subnet.
5) AD-Server: A Microsoft Active Directory Server which provides AAA (authentication, authorization and accounting) services for JS employees. → Because this is the basis of AAA security information, this is placed in the Intranet-Subnet.

6) WSA-Gateway: A Web Security Appliance, which provides a secure web application proxy.   Any JS employees connecting to any public Internet web servers (via either HTTP or HTTPS) must go through the WSA-Gateway for security. Employee browsers can only connect to Internet web servers by going through the WSA-Gateway. → Because this is needed by internal JS employees, this is placed in the Intranet-Subnet.

Please see the figure below for more details.



JS Network Server Placement and IPs

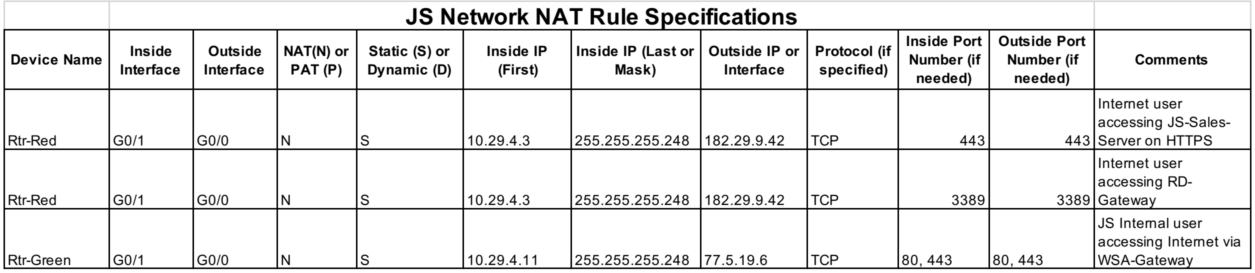
Server Name	Subnet Name	Server IP	Subnet Mask	Default Gateway IP
JS-Sales-Server	DMZ-Subnet	10.29.2.10	255.255.255.0	10.29.2.3
DB-Server	Intranet-Subnet	10.29.3.10	255.255.255.0	10.29.3.3
HR-Server	Intranet-Subnet	10.29.3.20	255.255.255.0	10.29.3.3
RD-Gateway	DMZ-Subnet	10.29.2.20	255.255.255.0	10.29.2.3
AD-Server	Intranet-Subnet	10.29.3.30	255.255.255.0	10.29.3.3
WSA-Gateway	Intranet-Subnet	10.29.3.40	255.255.255.0	10.29.3.3

V. Network Address Translation

A. Requirements and Implementation

Network Address Translation (NAT) is required for this network design. Since all the JS Network IP addresses are private, and there are only two public IP addresses assigned to the outside interface of each router, then all internal IP addresses need to be translated into one of the two public addresses to reach out to the Internet. I have assigned Rtr-Red and Rtr-Green to implement NAT translations so that each path translates its own paths' private IP addresses to the public IP address assigned to their outside interface.

Please see the below figure for additional details.



JS Network NAT Rule Specifications											
Device Name	Inside Interface	Outside Interface	NAT(N) or PAT (P)	Static (S) or Dynamic (D)	Inside IP (First)	Inside IP (Last or Mask)	Outside IP or Interface	Protocol (if specified)	Inside Port Number (if needed)	Outside Port Number (if needed)	Comments
Rtr-Red	G0/1	G0/0	N	S	10.29.4.3	255.255.255.248	182.29.9.42	TCP	443	443	Internet user accessing JS-Sales-Server on HTTPS
Rtr-Red	G0/1	G0/0	N	S	10.29.4.3	255.255.255.248	182.29.9.42	TCP	3389	3389	Internet user accessing RD-Gateway
Rtr-Green	G0/1	G0/0	N	S	10.29.4.11	255.255.255.248	77.5.19.6	TCP	80, 443	80, 443	JS Internal user accessing Internet via WSA-Gateway

B. Demonstration Examples

To demonstrate how NAT works, I will provide several scenarios and describe the route of the packets.

1) If an Internet user at public IP address 4.5.6.7 connects to JS-Sales-Server to order some nuts, then a packet is sent from the Internet user’s device (Source IP: 4.5.6.7, Destination IP: 182.29.9.42, Source Port: random, Destination Port: 443), through JS Network’s Rtr-Red and translated by NAT, and then forwarded through Firewall FW-R1 into the DMZ-Subnet and received by the JS-Sales-Server (Source IP: 4.5.6.7, Destination IP: 10.29.2.10, Source Port: random, Destination Port: 443).
2) If WSA-Gateway sets up a new HTTP connection to a public web server at IP address 22.3.4.5, then a packet is sent from the WSA-Gateway (Source IP: 10.29.3.40, Destination IP: 22.3.4.5, Source Port: random, Destination Port: 80), through Firewall FW-G1, and then out through Rtr-Green and NAT translated, and then received by the public web server (Source IP: 77.5.19.6, Destination IP: 22.3.4.5, Source Port: random, Destination Port: 80).
3) If an internal Client connects to HR-Server to check on their vacation time, then a packet is sent from the internal Client’s device (Source IP: private IP of Internal Client in the appropriate range designated, Destination IP: 10.29.3.20, Source Port: random, Destination Port: 80, 443), through Firewall FW-G2, and is received by the JS-HR-Server

(Source IP: private IP of Internal Client in the appropriate range designated, Destination IP: 10.29.3.20, Source Port: random, Destination Port: 80, 443). NAT translation is not needed in this scenario because both the Client and the Server on both on private IP addresses within the JS Network.

VI. Static Routes

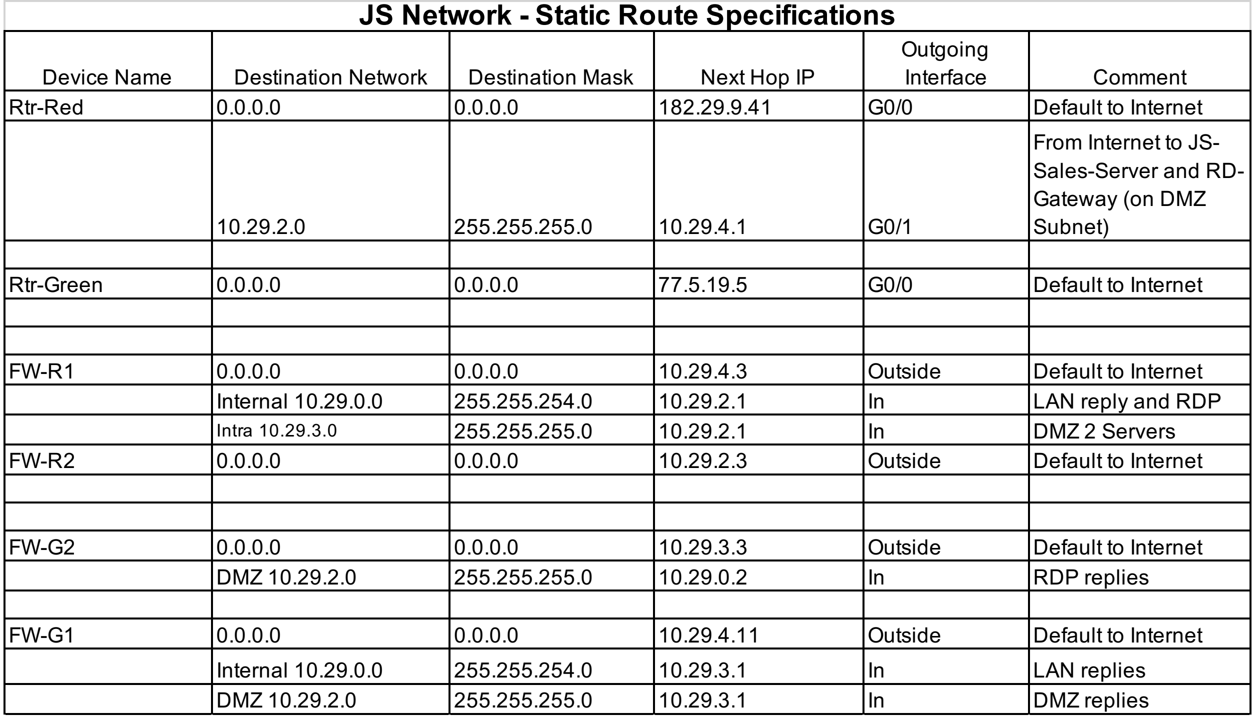
A. Default to Internet

A default static route is configured on each router and firewall to route traffic to the Internet.

B. Static Requirements

A static route is configured on certain routers and firewalls to allow all connections described in Section 1e of the Request For Proposal.

Please see the figure below for details on all default and static routes.



JS Network - Static Route Specifications

Device Name	Destination Network	Destination Mask	Next Hop IP	Outgoing Interface	Comment
Rtr-Red	0.0.0.0	0.0.0.0	182.29.9.41	G0/0	Default to Internet
	10.29.2.0	255.255.255.0	10.29.4.1	G0/1	From Internet to JS-Sales-Server and RD-Gateway (on DMZ Subnet)
Rtr-Green	0.0.0.0	0.0.0.0	77.5.19.5	G0/0	Default to Internet
FW-R1	0.0.0.0	0.0.0.0	10.29.4.3	Outside	Default to Internet
	Internal 10.29.0.0	255.255.254.0	10.29.2.1	In	LAN reply and RDP
	Intra 10.29.3.0	255.255.255.0	10.29.2.1	In	DMZ 2 Servers
FW-R2	0.0.0.0	0.0.0.0	10.29.2.3	Outside	Default to Internet
FW-G2	0.0.0.0	0.0.0.0	10.29.3.3	Outside	Default to Internet
	DMZ 10.29.2.0	255.255.255.0	10.29.0.2	In	RDP replies
FW-G1	0.0.0.0	0.0.0.0	10.29.4.11	Outside	Default to Internet
	Internal 10.29.0.0	255.255.254.0	10.29.3.1	In	LAN replies
	DMZ 10.29.2.0	255.255.255.0	10.29.3.1	In	DMZ replies

VII. Firewall Rules

A. One-Way Permission

The chosen dual-path dual-layer architecture allows all firewalls to be one-way permit firewalls where new connections are only allowed in one direction through the firewall. This is because the dual-path is structured to separate traffic – each path being dedicated to either incoming (left, “Red Rail”) or outgoing (right, “Green Rail”) traffic – which simplifies the Rulesets for each firewall. The left path only allows new TCP connections in the incoming direction, while the right path only allows new TCP connections in the outgoing direction. So, for every firewall, one interface will be “deny ip any any” because it will never need to initiate new connections in that direction. This greatly simplifies firewall management and enhances security.

B. Firewall Rules Requirements

To illustrate the Firewall Rules and Requirements needed for this design, I will list the requirements established in Section 1e of the Request For Proposal and describe what firewall rules will be needed to allow access. The JS Network must allow (permit) the following connections:

1. Connections to Sell Snacks:
    a. Internet users can connect to JS-Sales-Server using HTTPS over TCP → The firewall rule should allow incoming traffic on TCP port 443 to the IP address of the JS-Sales-Server (10.29.2.10)
    b. JS-Sales-Server can connect to DB-Server using the default PostgreSQL TCP port to submit web sales orders. → The firewall rule should allow outgoing traffic from the JS-Sales-Server IP address (10.29.2.10) to the DB-Server IP address (10.29.3.10) on TCP port 5432 (the default PostgreSQL port).
    c. JS Internal Clients can connect to DB-Server using the default PostgreSQL TCP port to enter sales orders received over the telephone into the database. → The firewall rule should allow outgoing traffic from the Internal Network to the DB-Server IP address (10.29.3.10) on TCP port 5432 (the default PostgreSQL port).
2. Connections for Employee Logins and HR:
    a. JS Internal Clients can connect to AD-Server using default TCP port for Lightweight Directory Access Protocol (LDAP) to authenticate user logins. → The firewall rule should allow outgoing traffic from the Internal Network to the AD-Server IP address (10.29.3.30) on TCP port 389 (the default LDAP port).

b. Internet users can connect to RD-Gateway using default TCP port for Remote Desktop Protocol (RDP). → The firewall rule should allow incoming traffic on TCP port 3389 (the default port for RDP) to the IP address of the RD-Gateway (10.29.2.20).

c. RD-Gateway can connect to AD-Server using default TCP port for Lightweight Directory Access Protocol (LDAP) to authenticate user logins. → The firewall rule should allow outgoing traffic from the RD-Gateway IP address (10.29.2.20) to the AD-Server IP address (10.29.3.30) on TCP port 3389 (the default port for RDP).

d. RD-Gateway can connect to JS Internal Client Workstations using RDP over TCP. → The firewall rule should allow outgoing traffic from the RD-Gateway IP address (10.29.2.20) to the Internal Network on TCP port 3389 (the default port for RDP).

e. JS Internal Client Workstations can connect to HR-Server using HTTPS over TCP. → The firewall rule should allow outgoing traffic from the Internal Network to the HR-Server IP address (10.29.3.20) on TCP port 443.

3. Connections for Employee web access:

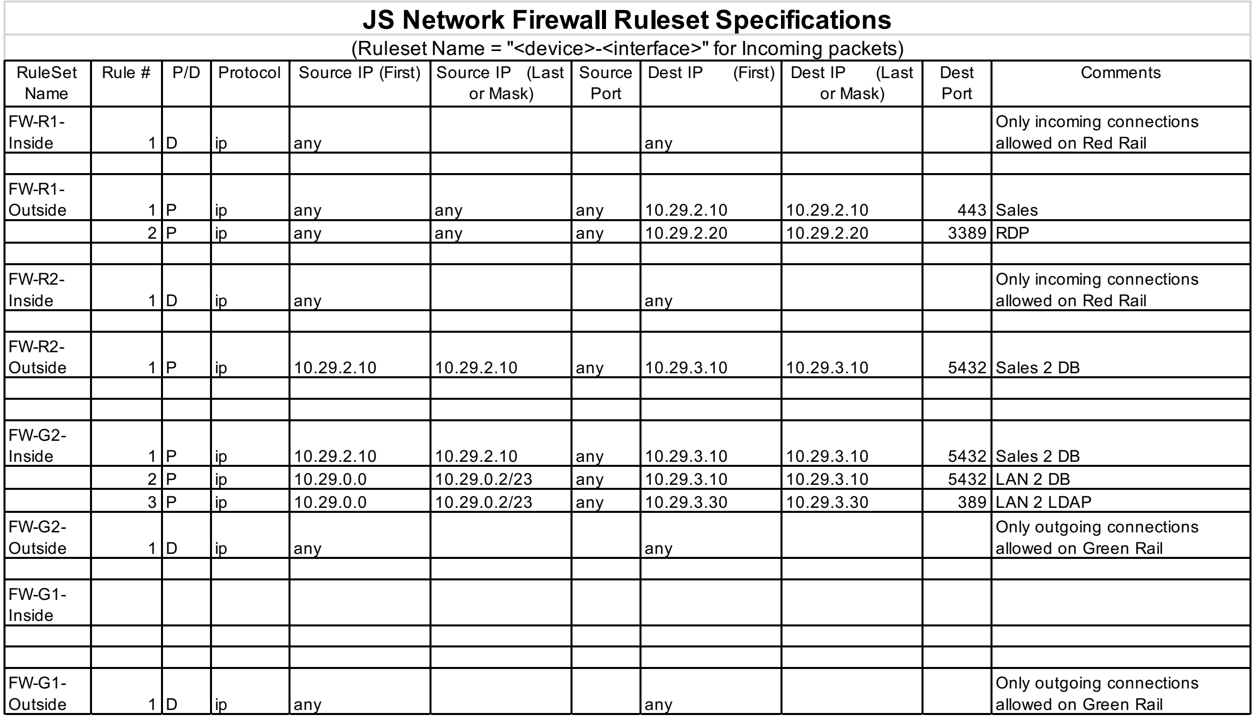
   a. JS Employees can connect to WSA-Gateway using HTTP or HTTPS over TCP to request an outgoing connection to a web server on the public Internet. → The firewall rule should allow outgoing traffic from the Internal Network to the WSA-Gateway IP address (10.29.3.40) on TCP ports 80 and 443.

   b. WSA- Gateway can connect to any public Internet web server using HTTP or HTTPS over TCP. → The firewall rule should allow outgoing traffic from the WSA-Gateway (10.29.3.40) to any IP on TCP ports 80 and 443.

4. All connections that are not permitted above are denied. → This is achieved by the default deny rule, mentioned above, that blocks all traffic that does not match any of these rules.

C. Definitions

Please see the figure below for the JS-Ruleset-Definition Table.



JS Network Firewall Ruleset Specifications

(Ruleset Name = "<device>-<interface>" for Incoming packets)

RuleSet Name	Rule #	P/D	Protocol	Source IP (First)	Source IP (Last or Mask)	Source Port	Dest IP (First)	Dest IP (Last or Mask)	Dest Port	Comments
FW-R1-Inside	1	D	ip	any			any			Only incoming connections allowed on Red Rail
FW-R1-Outside	1	P	ip	any	any	any	10.29.2.10	10.29.2.10	443	Sales
	2	P	ip	any	any	any	10.29.2.20	10.29.2.20	3389	RDP
FW-R2-Inside	1	D	ip	any			any			Only incoming connections allowed on Red Rail
FW-R2-Outside	1	P	ip	10.29.2.10	10.29.2.10	any	10.29.3.10	10.29.3.10	5432	Sales 2 DB
FW-G2-Inside	1	P	ip	10.29.2.10	10.29.2.10	any	10.29.3.10	10.29.3.10	5432	Sales 2 DB
	2	P	ip	10.29.0.0	10.29.0.2/23	any	10.29.3.10	10.29.3.10	5432	LAN 2 DB
	3	P	ip	10.29.0.0	10.29.0.2/23	any	10.29.3.30	10.29.3.30	389	LAN 2 LDAP
FW-G2-Outside	1	D	ip	any			any			Only outgoing connections allowed on Green Rail
FW-G1-Inside										
FW-G1-Outside	1	D	ip	any			any			Only outgoing connections allowed on Green Rail

VIII. Modifications for High-Availability Service

A. High-Availability Solutions

For High-Availability Service that allows Internet users to still place orders on the JS-Sales-Server even if one switch, link, or firewall fails, there are several modifications that can be made to this dual-path dual-layer design. For switches, we can use the Spanning Tree Protocol (STP). STP is a network protocol that builds a logical loop-free topology for Ethernet networks. It prevents network loops that can result in broadcast issues. By using STP, we could have redundant paths between switches, but only one active path at a time. Regarding firewalls, we can use firewall clusters. A firewall cluster is a group of firewalls that work together to provide increased availability and reliability. If one firewall fails, the others can take over. We can use Virtual IP services to allow the firewalls in the cluster to share a single IP address so that if one fails, the IP address will still be reachable via the other firewalls.

B. Active/Active vs. Active/Passive

There are two main types of firewall cluster configurations: Active/Active and Active/Passive. In an Active/Active configuration, all firewalls in the cluster are actively processing traffic. This configuration provides load balancing since the traffic load is distributed across multiple firewalls. The disadvantage here is that this configuration is more complex to set up and manage. In an Active/Passive configuration, one firewall (active) processes all traffic, while the other firewalls (passive) are on standby in case the active firewall fails. Upon failure of the active firewall, one of the passive firewalls is elected to take over. While this configuration is simpler to set up and manage, it does not provide load balancing like the Active/Active configuration.

IX. Conclusion

In conclusion, this dual-path dual-layer network design is an optimal choice for the JS Network. As discussed, it provides load balancing, separation of duties, enhanced security, redundancy, high availability, and scalability. The architecture's high availability and reliability makes it so traffic is balanced across two paths and if one path fails, the other can take over. This design can add additional devices to each path if needed. Additionally, the dual layers of firewalls provides an additional defense against potential threats to the Internal Network. Furthermore, the one-way permit firewall configuration simplifies management. Overall, this design can effectively support the current and future needs of the JS Network.

References:

Cisco. (2023, January 6). *What is high availability?*. Cisco. https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-high-availability.html

Cisco. (n.d.). *Cisco Press*. Hierarchical Network Design Overview (1.1) > Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design | Cisco Press. https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4

Huston, B., Huston, B., 4, lbhuston on F., 4, infosectony on F., 4, T. on F., 4, M. on F., 5, T. on F., 5, K. on F., & 5, lbhuston on F. (2016, February 4). *Comparing 2 models for DMZ implementations*. MSI :: State of Security. https://stateofsecurity.com/comparing-2-models-for-dmz-implementations/

Kaseya. (2021, August 10). *High availability: What it is and how you can achieve it*. Kaseya. https://www.kaseya.com/blog/2021/08/10/high-availability/

Syeda Famita Amber. May 13th, Chawla, D., Ramachandran, A., & Faraz, M. (2022, December 29). *Understanding active-active clustering: A comprehensive guide 101 - learn*. Hevo. https://hevodata.com/learn/active-active-clustering/

Tech2020. (2020, September 22). *DMZ Networks - ITperfection - Network Security*. ITperfection. https://www.itperfection.com/networking/dmz-networks-security-firewall-subnettig-vlan/