

Data Security

A Secure Network Architecture

3-28-2022

AVERY JAN



Introduction

For companies like healthcare companies that process a fair amount of personal and confidential information of their customers, secure data transmission over their network is vital to their businesses. This project proposes a secure network architecture that ensures the data security while meeting the business requirements of those companies. Several crucial features that are built into the architecture to guard the network include redundancy at edge, internal traffic flow reduction by moving some services to Cloud, compartmentalization of the network core, and multiple layers of protection devices and software throughout. There are three main sections in the architecture. Section One is the part of the network from the outer edge of the network to the outer firewall. Section Two encompasses the part of the network between the two firewalls. Section Three starts at the inner firewall and extends to the innermost part of the network (the core). The strategies for constructing each section and the types of components are discussed. A layout for placing intrusion detection/prevention systems within the network to fortify it is provided and a plan for assigning public and private IP addresses is offered. The vendors for the components of the architecture, the anti-virus and anti-malware for each system/device that connects to the network as well as identity management and log management are recommended.

Outline

- **Introduction**
- **Business requirements**
- **Terminology**
- **Architecture of the security network**
- **Sections of the security network**
 - (1) From the edge of the network to outer firewall
 - (2) Between the outer firewall and the inner firewall
 - (3) From the inner firewall to internal network
- **IP Address Plan**
- **Recommendations** for hardware, software, and services (Cloud, etc.)
- **Identity management and log management**
- **Anti virus and anti malware**
- **Summary**

Business Requirements

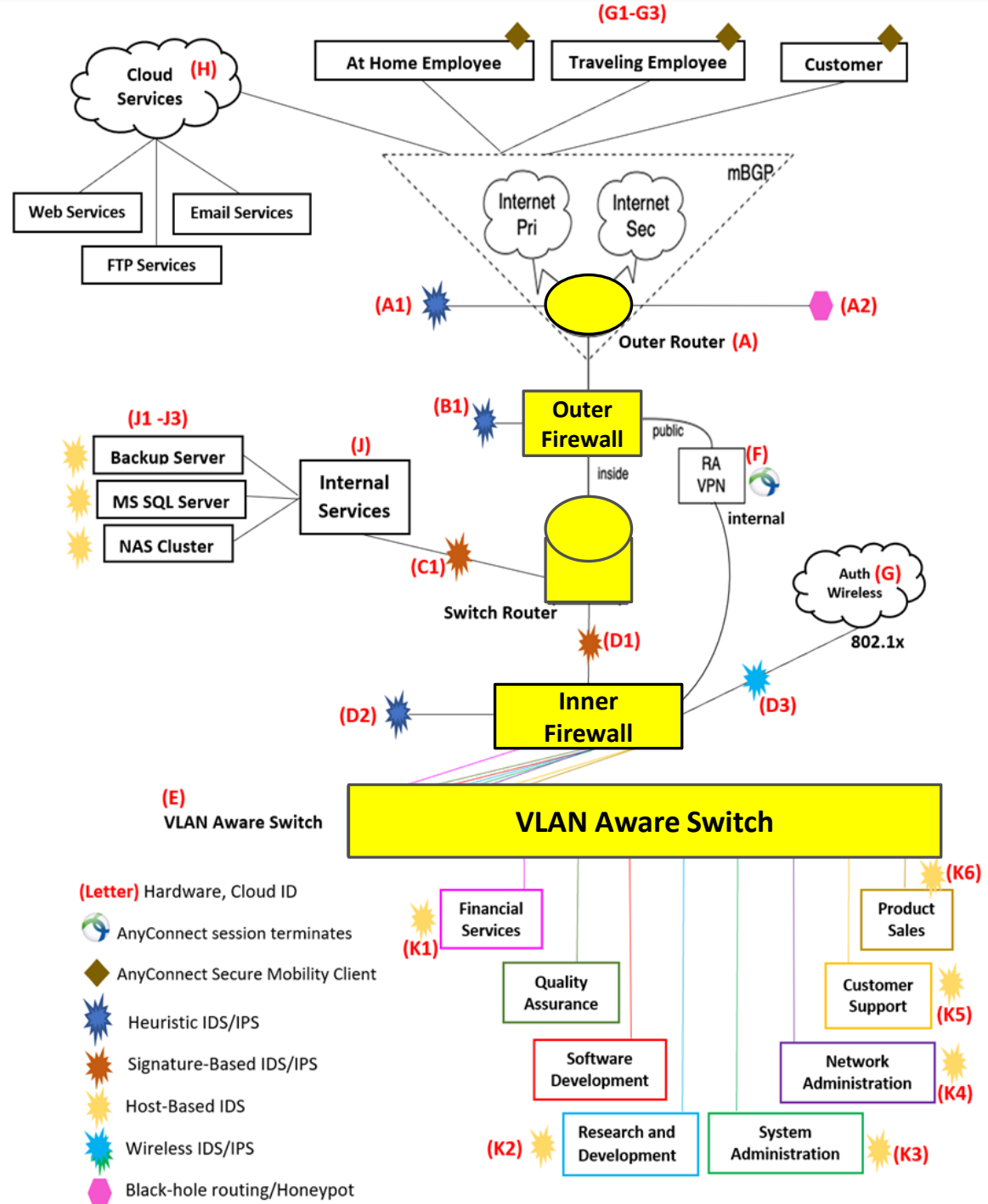
1. Core services need to be available to all groups in one form or another.
2. Company users need to be able to reach the internal resources from the road (while visiting customers) and from home remote workers.
3. Customers need to be able to communicate with the company via e-mail.
4. Customers need to be able to access information on both the web server and the FTP server.
5. Development groups need to be able to move software to the QA group for analysis.
6. Customer support and sales need to be able to interact with customers outside the network infrastructure.
7. Network administration and system's administration have access to computers and network equipment to managing them.
8. Financial systems are to be isolated from everyone else, but financial group still has access to core services and the Internet.
9. Redundancy and resiliency are important services for all users.

The Architecture

Segmentation and Isolation

The backbone

- Outer Router
- Outer Firewall
- Switch Router
- Inner Firewall
- VLAN Aware Switch



Terminology

The Architecture

- **Network Segmentation** is a network security technique that divides a network into smaller, distinct sub-networks that enable network teams to compartmentalize the sub-networks and deliver unique security controls and services to each sub-network.
- **Network Isolation** is the segmenting of a computer network into separate zones with distinct trust levels, for the purpose of containing hazards or reducing damage caused by a threat actor.
- **Network compartmentalization** is the limiting of access to information to persons or other entities on a need-to-know basis to perform certain tasks.
- **Router** is a networking device that forwards data packets between computer networks.
- **Firewall** is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.
- **VLAN** (virtual local area network) is a virtualized connection that connects multiple devices and network nodes from different LANs into one logical network.
- **A VLAN Aware switch** is the virtual switch enforces the VLAN defined topology constructed by the LAN administrator.
- **Switch Router** is a router that has dual functions (1) connecting to a VLAN Aware switch that tags and un-tags VLANs on different switch-ports (2) route traffic to desirable destinations.

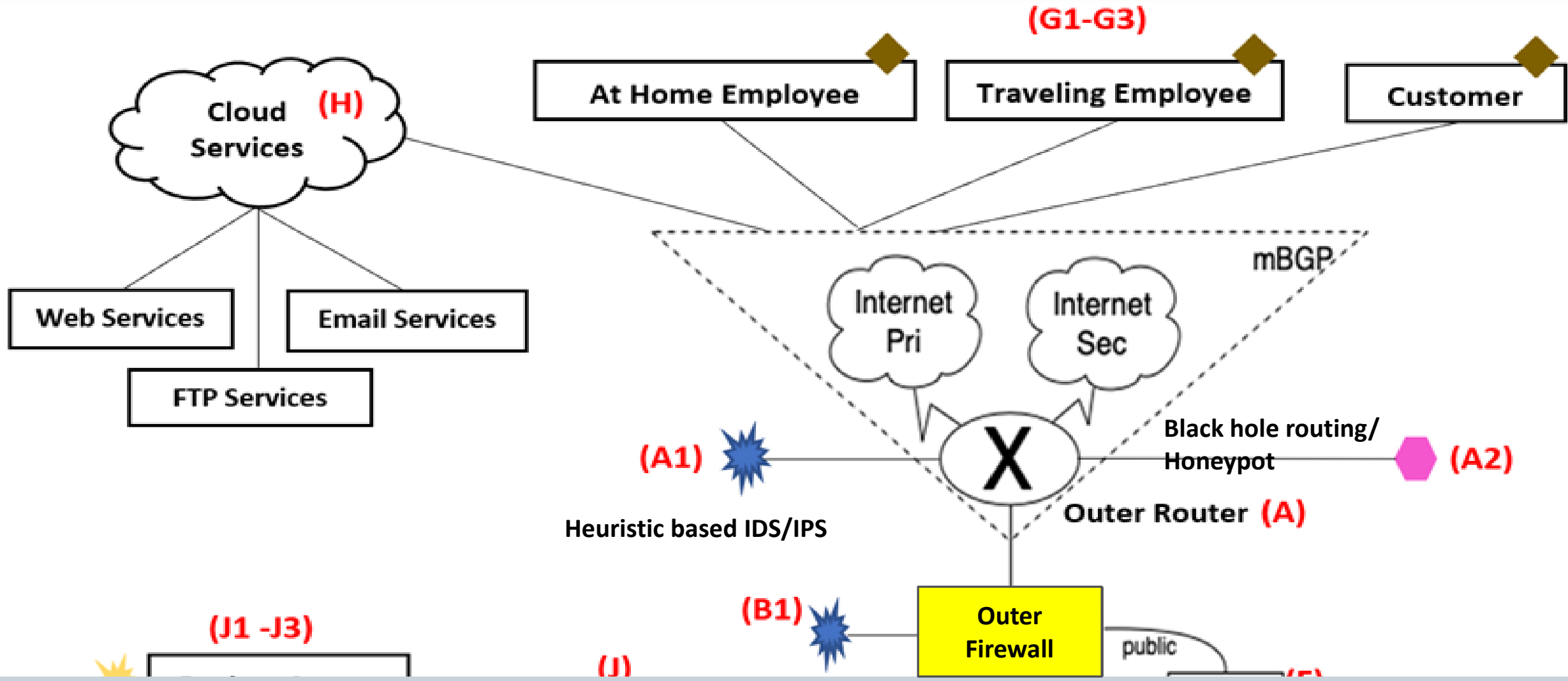
**From
The Edge
to
Outer Firewall**

Strategy From the Edge to Outer Firewall

1. Move as many services to Cloud as possible: Web, FTP, and email services.
2. Block as much unwanted traffic from outside as possible using the following:
 - **Dual Internet Connections** provide redundancy and resiliency to minimize network downtime.
 - **mBGP** (Multi-protocol Extensions) for BGP is an extension to Border Gateway Protocol (BGP) that allows different types of addresses (known as address families) to be distributed in parallel.
 - **Heuristic-based IDS/IPS** focuses on detecting intrusions by monitoring the activities of systems and classifying them as normal or anomalous.
 - **Black Hole Routing** means that a router directs network traffic to a destination that just “throws away” the traffic.
 - **Honeypot** is a cybersecurity mechanism that uses a manufactured attack target to lure cyber-criminals away from legitimate targets.
 - **Outer Firewall/External Firewall** monitors the network's perimeter and prevents unauthorized access from the outside.

From the Edge to Outer Firewall

- Dual Internet Connections
- Heuristic-based IDS/IPS, Black Hole Routing
- Outer Router, mBGP
- Honeypot
- Outer Firewall



**Between
Outer Firewall
and
Inner Firewall**

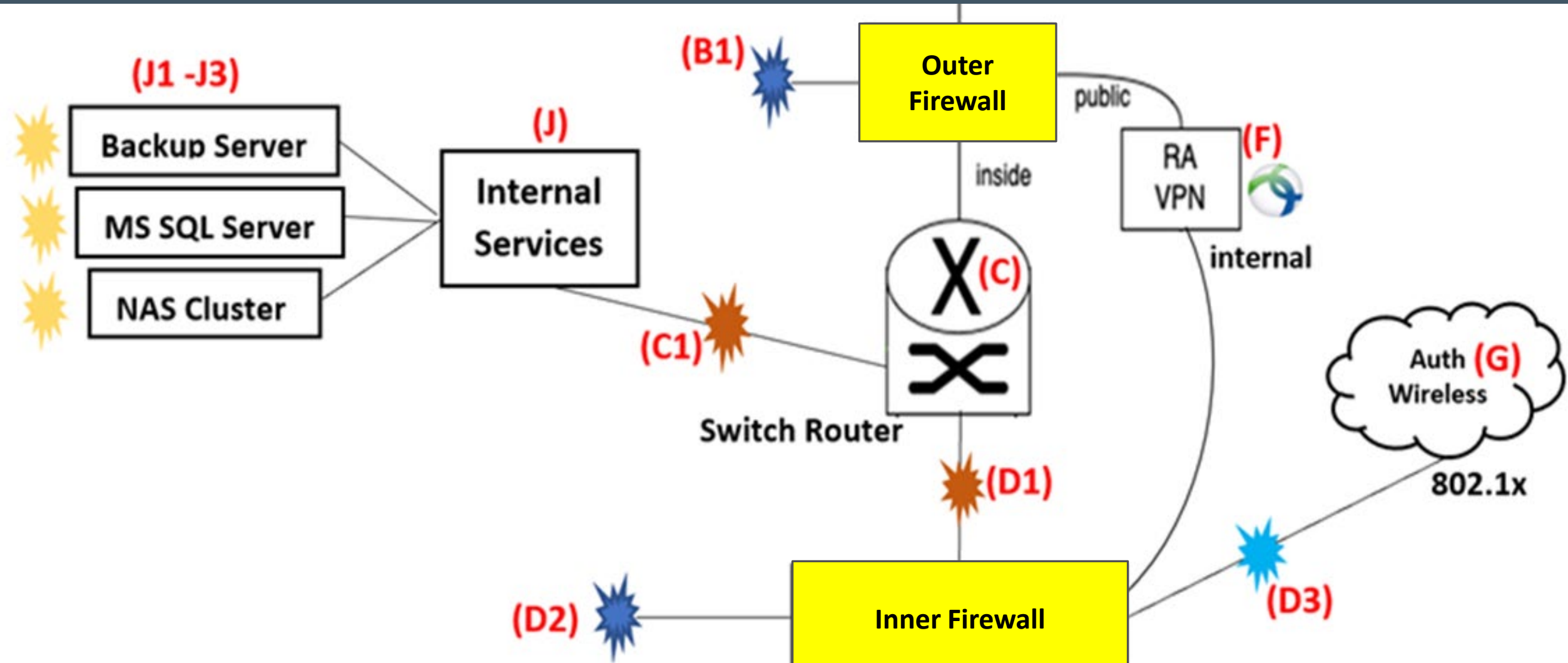
Strategy Between Outer Firewall and Inner Firewall

1. Ensure remote employees securely access the network.
2. Authenticate wireless users for accessing internal services.
3. Implement a switch router ahead of compartmentalizing the internal network.
 - **Remote Access VPN (RA VPN on diagram)** A remote access virtual private network (VPN) enables users who are working remotely to securely access and use applications and data that reside in the corporate data center and headquarters, encrypting all traffic the users send and receive.
 - **Authorization of Wireless Users** This is accomplished by using Extensible Authentication Protocol (EAP) framework that can add new authentication options and is integrated with 802.1X port-based access control, an IEEE Standard for port-based Network Access Control.
 - **Switch Router** is a device that combines the abilities of both switches and routers for routing data around and between networks. This device is able to forward data based on a device's physical address, as a switch, as well as forward packets based on the location of the next hop address as a router. o desirable destinations

Between Outer Firewall and Inner Firewall

Outer & Inner Firewalls
Remote Access VPN

Switch Router
Authorization of Wireless Users



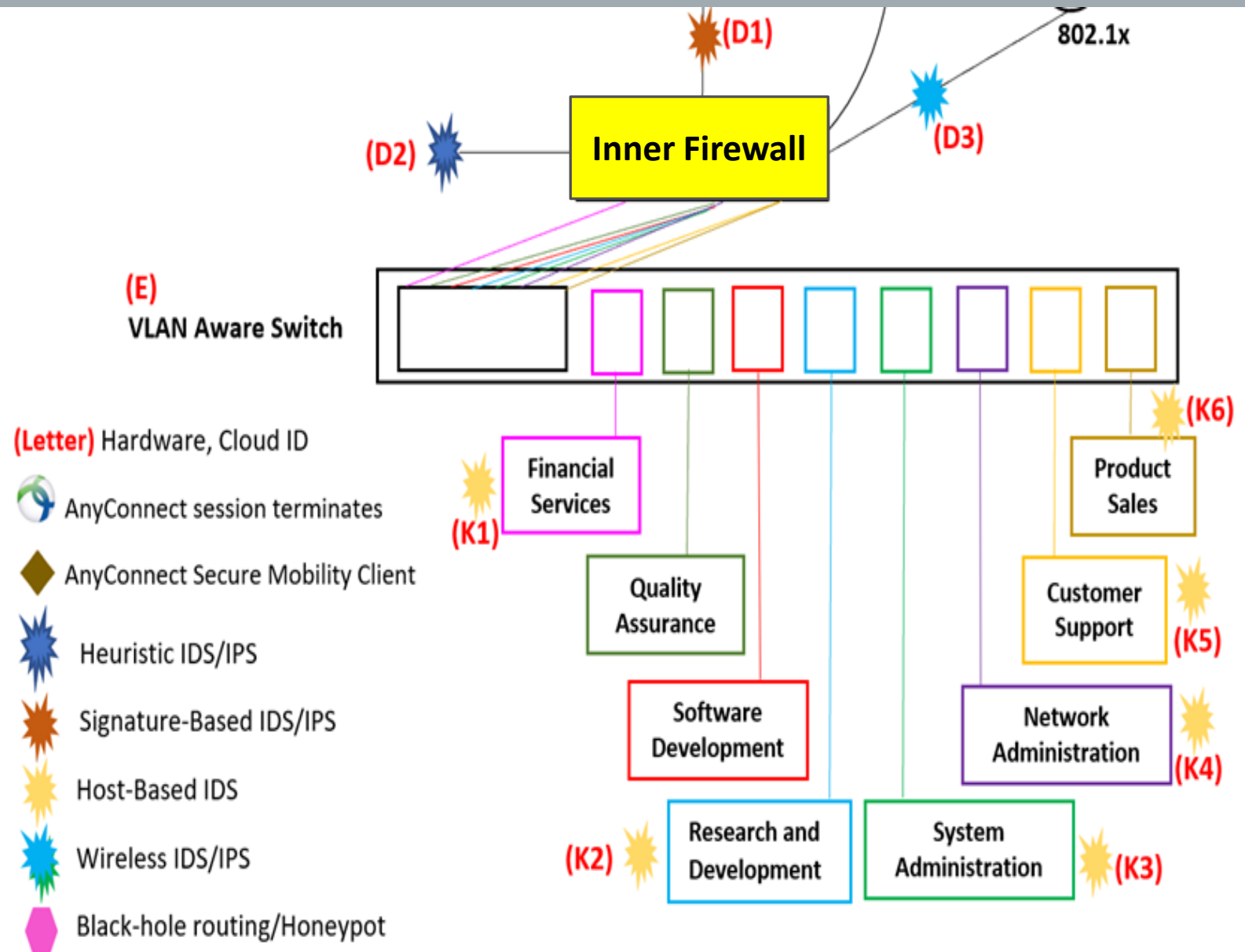
**From
Inner Firewall
to
Internal Network**

Strategy From Inner Firewall to Internal Network

1. Compartmentalize internal departments.
2. Ensure the rightness of incoming and outgoing traffic of internal network.
3. **Firewall** is a device or software designed to monitor traffic and prevent unauthorized access, and an internal firewall is an advanced application of that concept.
4. **Inner Firewall or Internal Firewall** is a security solution designed to protect a network from attacks that have already gotten past the perimeter.
5. **VLAN Aware Switch** a physical network of devices can be segmented into multiple domains. A VLAN Aware Switch places the traffic from hosts and wireless networks in different VLANs. The VLAN Aware switch feature allows the Edge Router to tag and untag VLANs on different switch-ports.

From Inner Firewall to Internal Network

- Inner Firewall
- VLAN Aware Switch
- Access to Desktops
- Signature-based IDS/IPS
- Heuristic-based IDS/IPS
- Host-based IDS/IPS
- WIDS/WIPS



Intrusion Detection Systems and IP Address Plan

Strategy



Intrusion Detection System/Intrusion Prevention System

Use intrusion detection systems at various spots of the network to continuously monitor the network for malicious activity or policy violations. If an intrusion prevention system is installed, it will take actions like reporting, blocking, or dropping it to prevent the malicious activity from reoccurring.

- **Signature-based IDS/IPS** monitors packets in a network and compares it with pre-configured and pre-determined attack patterns known as signatures.
- **Heuristic-based IDS/IPS** focuses on detecting intrusions by monitoring the activity of systems and classifying it as normal or anomalous using heuristics or rules to detect misuse, rather than patterns or signatures.
- **Host-based IDS/IPS** is a program that monitors the characteristics of a single host and the events occurring within that host to identify and stop suspicious activity.
- **WIDS/WIPS** is a network device that monitors the radio spectrum for the presence of unauthorized access points, and can automatically take countermeasures.

Intrusion Detection Systems throughout the Network

NIDS/NIPS

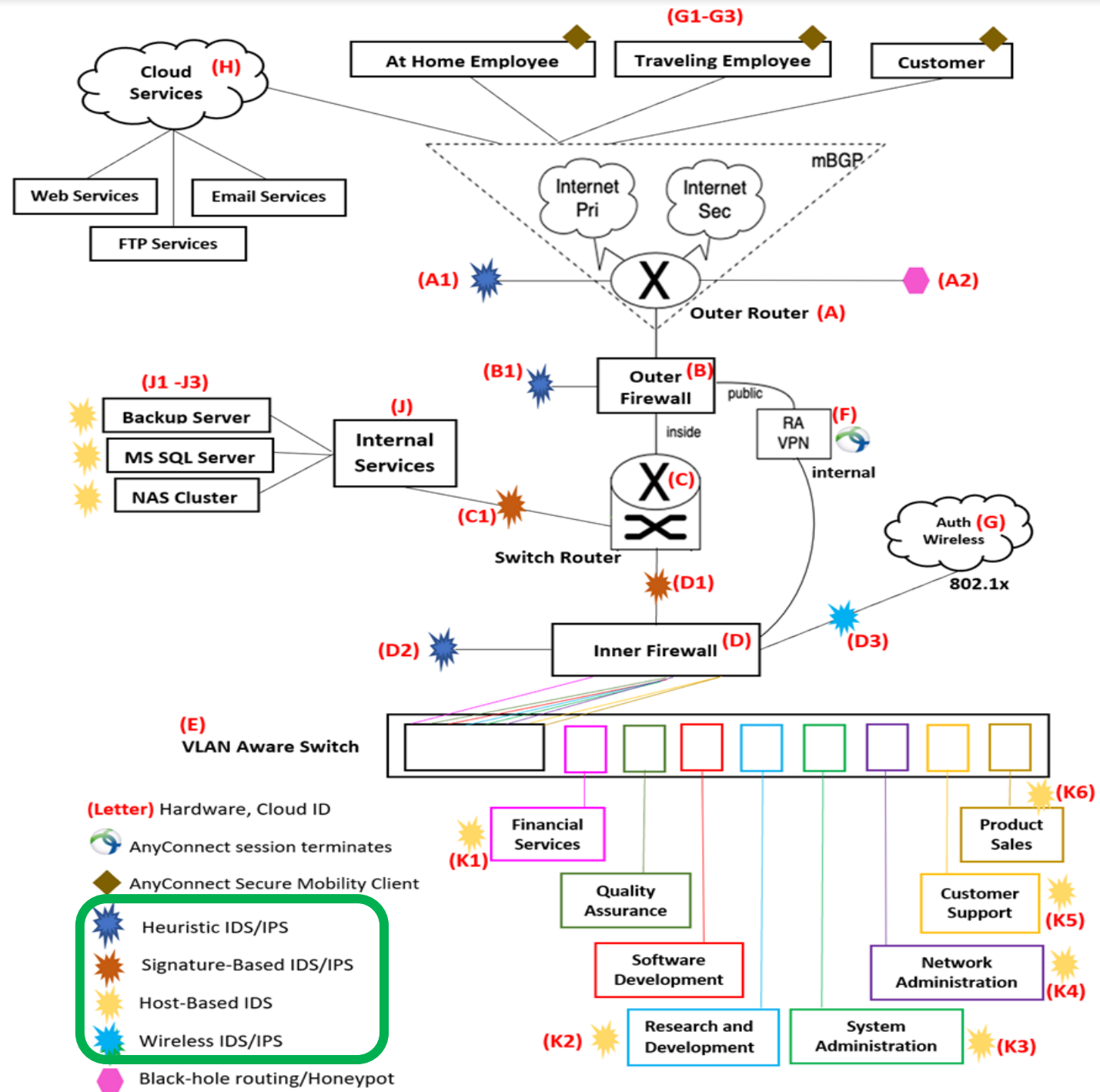
- Heuristic-based 
- Signature-Based 

HIDS

Servers & Desktops 

WIDS/WIPS

Authorization of wireless users 



IP Addressing Plan

Address in green

Public IP Address

79.12.40.0/30

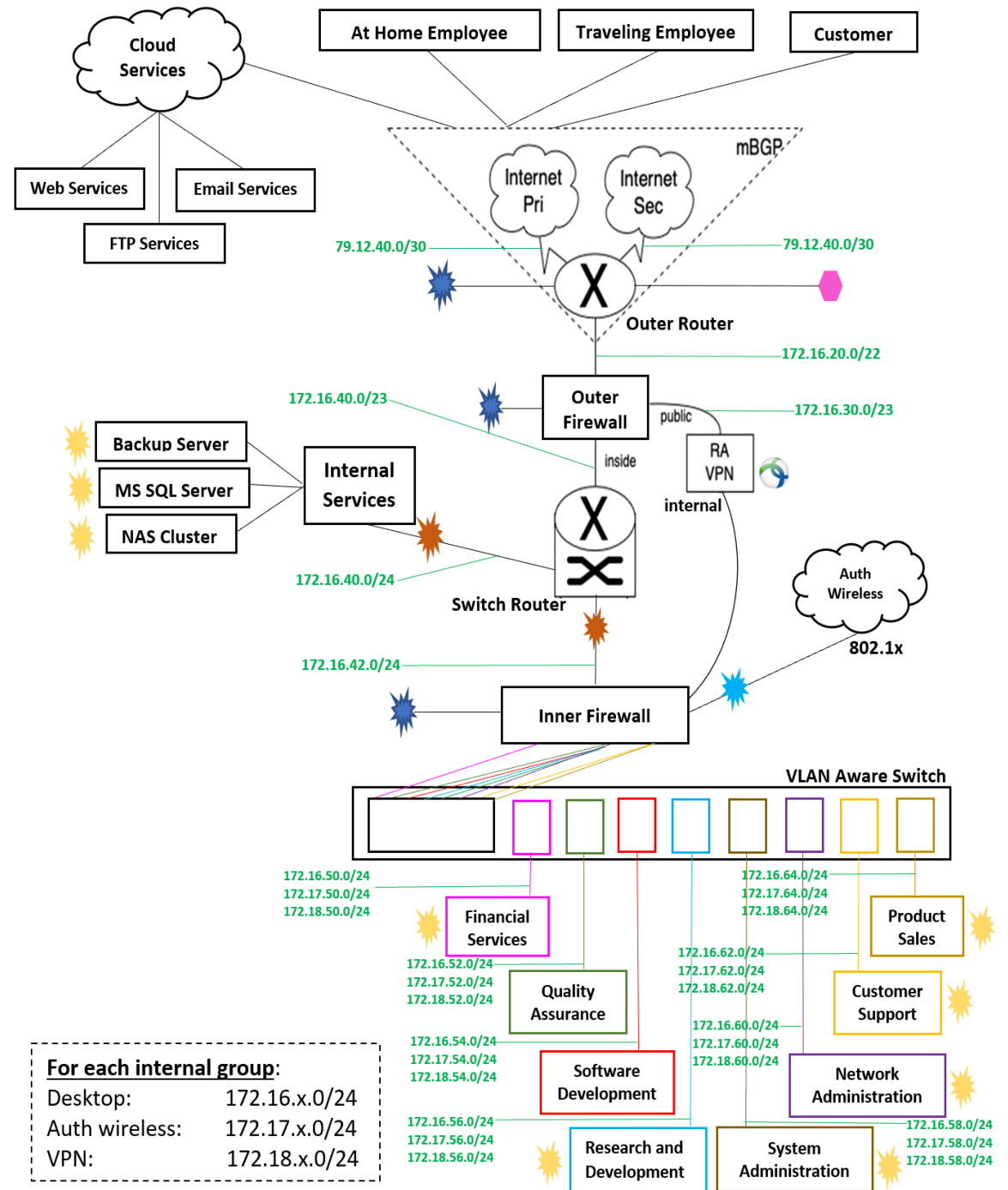
Private IP Addresses:

RFC 1918

172.16.x.0/x

172.17.x.0/24

172.18.x.0/24



Recommendations

Hardware, Software, and Services

Outer Router & Heuristic-based IDS

Outer Router: *Juniper MX 480 Router*

- Maximum system throughput: 9 Tbps
- Flexible interface rates: 10GbE, 40GbE, and 100GbE.
- Support for Multiprotocol BGP (mBGP)
- Flow monitoring and video monitoring.

Heuristic-based IDS: *Zeek (aka Bro)*

- Proactively detect anomalies and suspicious signatures
- Track DNS, HTTP, and FTP activities and SNMP traffic
- Policy engine allows customized automation

Cloud Services (Web Services, FTP Services, Email Services)

Web Services: *Microsoft Azure, Content Delivery Network*

- Global coverage and massive scalability
- Handles sudden traffic spikes and heavy load
- High security (DDoS, HTTPs)

FTP Services: *Microsoft OneDrive*

- Protection from file loss
- Access selected files without being online

Email Services: *Microsoft Exchange Online*

- *group policies and other administration tools, to manage Exchange Online features across their environment.*

Firewalls & Remote Access VPN

Outer Firewall & Remote Access VPN: *Cisco ASA-5555*

- Firewall throughput: 4 Gbps
- Concurrent firewall connections: 1 million
- New connections per second: 22,000
- Cisco Security Intelligence: IP, URL, and DNS threat intelligence
- Centralized configuration, logging, monitoring, and reporting

Inner Firewall: *Fortinet FortiGate 2200 E (NGFW)*

- NSS Labs Recommended and ICSA validated security and performance
- Firewall Throughput: 150 Mpps
- TLS 1.3 deep inspection
- SSL Inspection Throughput (IPS, avg. HTTPS): 17 Gbps
- SSL Inspection Concurrent Session (IPS, avg. HTTPS): 2.5 Million

Switch Router & Authentication

Switch Router: *Cisco 9600 series*

- Purpose-built 40 and 100 Gigabit Ethernet line of modular switches targeted for the enterprise campus.
- Switching capacity of up to 25.6 Tbps
- Deliver the following tables: MAC, route, and Access Control List [ACL]
- Nonstop Forwarding with Stateful Switchover

Remote Access VPN Authentication Service: *Cisco AnyConnect*

- Integration of Duo with Cisco AnyConnect provides MFA authentication
- Protects company's network and devices against malware, viruses, and other cyber threats.

Wireless Users Authentication: *802.1x*

VLAN Aware Switch, Signature Based IDS/IPS, HIDS

VLAN Aware Switch: *Cisco 9600 series*

- The same type of hardware as the one used for the Switch Router

Signature-based IDS/IPS: *Cisco Firepower NGIPS 4145*

- NSS Labs tests: Effectiveness, 99.7% in stopping threats/100% in identifying evasion techniques
- Throughput, NGIPS (1024B): 55 Gbps
- Maximum concurrent sessions: 30 Million
- URL Filtering: 80 categories and URLs categorized, 280 million individual URLs
- 600 billion emails, > 1 billion web queries, and nearly 1.5 million malware samples daily

HIDS: *OSSEC*

- Applicable to all internal servers and various desktops
- Log analysis, integrity checking, rootkit detection, time-based alerting, and active response

Antivirus and Antimalware

Linux *Kaspersky*

Mac *Norton 360 Deluxe (for Mac), Bitdefender Antivirus for Mac, and Kaspersky Internet Security for Mac.*

Windows 11 *Bitdefender, Webroot, McAfee, ESET, G Data*

Windows 10 *Avast, AVG, Bitdefender, Kaspersky, Sophos*

Windows 8 *Avast, AVG, ESET, Kaspersky, Panda*

Identity Management & Log Management

Identity Management: *Microsoft Azure Active Directory*

- Authentication: Multi-factor authentication
- Custom banned password list and smart lockout
- Single Sign-On: Centralizes management of pre-integrated SaaS apps, plus custom and on-premises line-of-business apps

Log Management: *Splunk*

- Data collection & indexing, search capability, event correlation, and alerts.
- Used by many organizations for security monitoring, advanced threat detection, incident investigation and response.
- A “Leader” in Gartner’s 2020 Magic Quadrant (MQ) for (SIEM)
- Ranked the highest overall ability to execute.

Summary

A secure network architecture that protects a network from the edge all the way to the core of the network is presented. At the edge of the network, the focus is on ensuring that the connection with the outside world is reliable and safe by providing redundancy and blocking illegitimate traffic. In addition, web, file, and email services are moved to Cloud to reduce the traffic near the crucial internal network. Once the incoming traffic passes through the outer router, a double firewall setup serves as a shield against attacks on the internal network. Between these firewalls, remote access VPN, authorization of wireless users, and directing the traffic to internal servers take place to control the access to the inner firewall. The traffic that comes off the inner firewall is sent to a VLAN aware switch that directs the traffic to the compartmentalized internal network. A variety of intrusion detection/prevention systems are placed throughout the network for additional protection. Anti-virus/anti-malware are recommended for devices connected to the network. An IP plan that separates the public IP address from private IP addresses is proposed. Identity and log management are suggested for facilitating ongoing monitoring of the health of the network. Prominent vendors of the components of the architecture are provided.