Project Title: WORK FROM HOME BY REMOTE ACCESS VPN
Team name: unstoppables
Team leader name: Saranya Nedumaran
College name: Jbas college for women

Theme: Internet security

Problem Statement: 1. Due to lockdown employees that work from home often would do so from their personal computers which are significantly less secure than the organizational ones, making them more vulnerable to email attacks. The vast majority of which include advanced capabilities such as malicious Macros and exploits or redirection to malicious websites – a challenge that surpasses the capabilities of most Antiviruses and email protection solutions. Make a platform that detects if a link is malicious or not and keeps the user safe from downloading suspicious files or applications from the internet.

Idea / Approach

Describe your idea/approach: Most of the attacks not only by email attacks but also it was done by networks like vpn(virtual private network).The vpn is one of the mostly attacking area where the hackers can easily attack by using this method called man-in-the-middle-attack.Which can hack a particular sessions or particular private network without sending any mails or etc... There is a way that the company can create a separate vpn by their own without an programming language and they can host it into google cloud and any other .But most of the companies doesn’t know By the way it is hard to hack because the bandwidth oth google will be like 100gigs or may be more than that But the google has the most fastest bandwidth in the world so it’s hard to hack

Technology Stack and Use Cases

LIST ALL THE TOOLS AND TECHNOLOGIES USED TO BUILD AND RUN YOUR APPLICATION :

SECURITY SOFTWARE FOR USERS :

● BitDefender Total Security Multidevic

●Kaspersky Total Security McAfee Live safe.

ASA FIREWALL SOFTWARE

●Cisco ASDM for ASA

FEATURES BY ASA :

◆ Network client access ◆ AAA / local servers ◆ Host scan image

◆ Secure desktop manager.◆ DNS

ADVANCED :

◆ Connection gateway ◆ SSL settings ◆ Certificate to SSL vpn

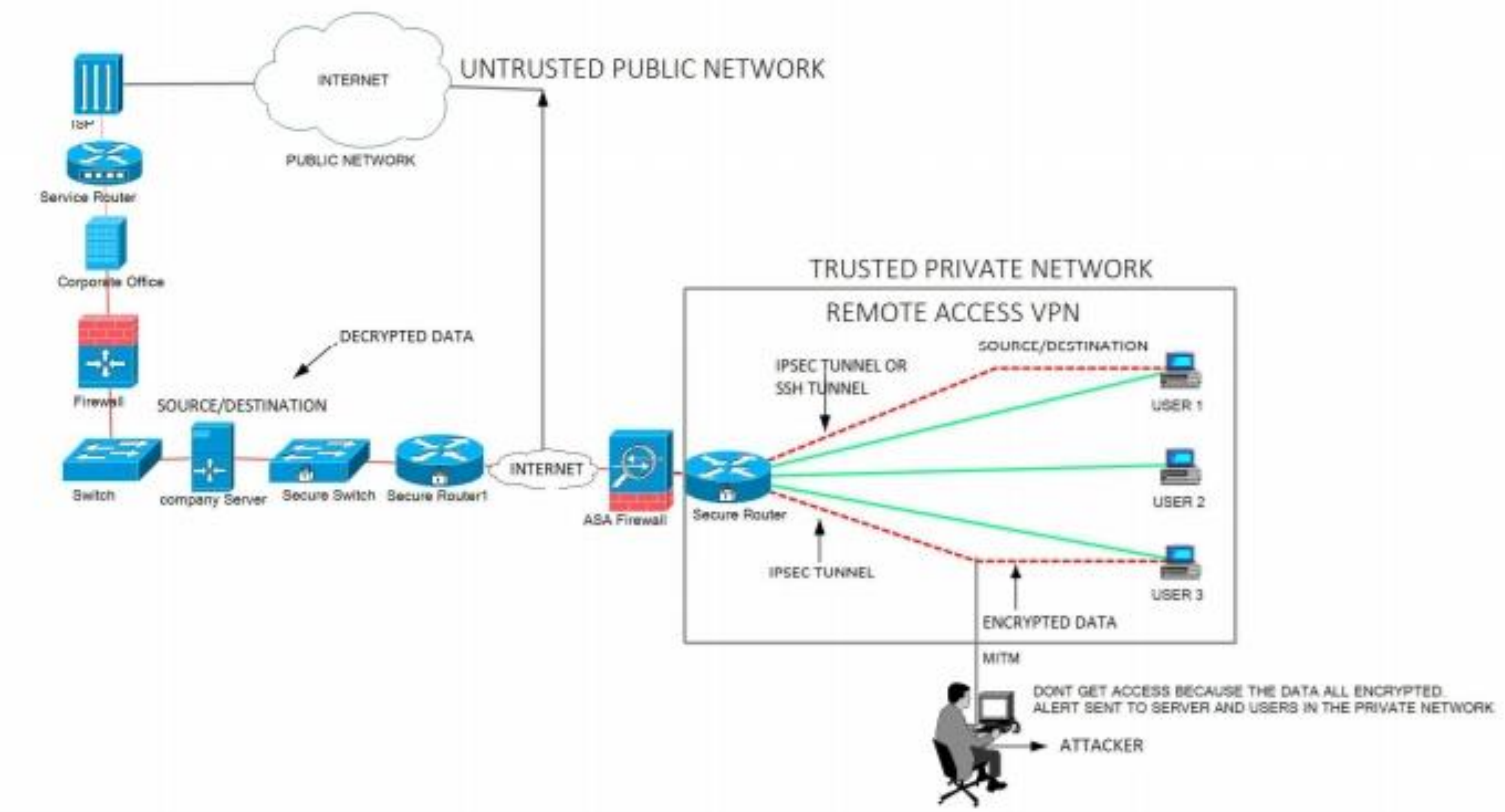
◆ HTTP redirect ◆ Email proxy

Describe Your Use Cases Here Security Software For Users :

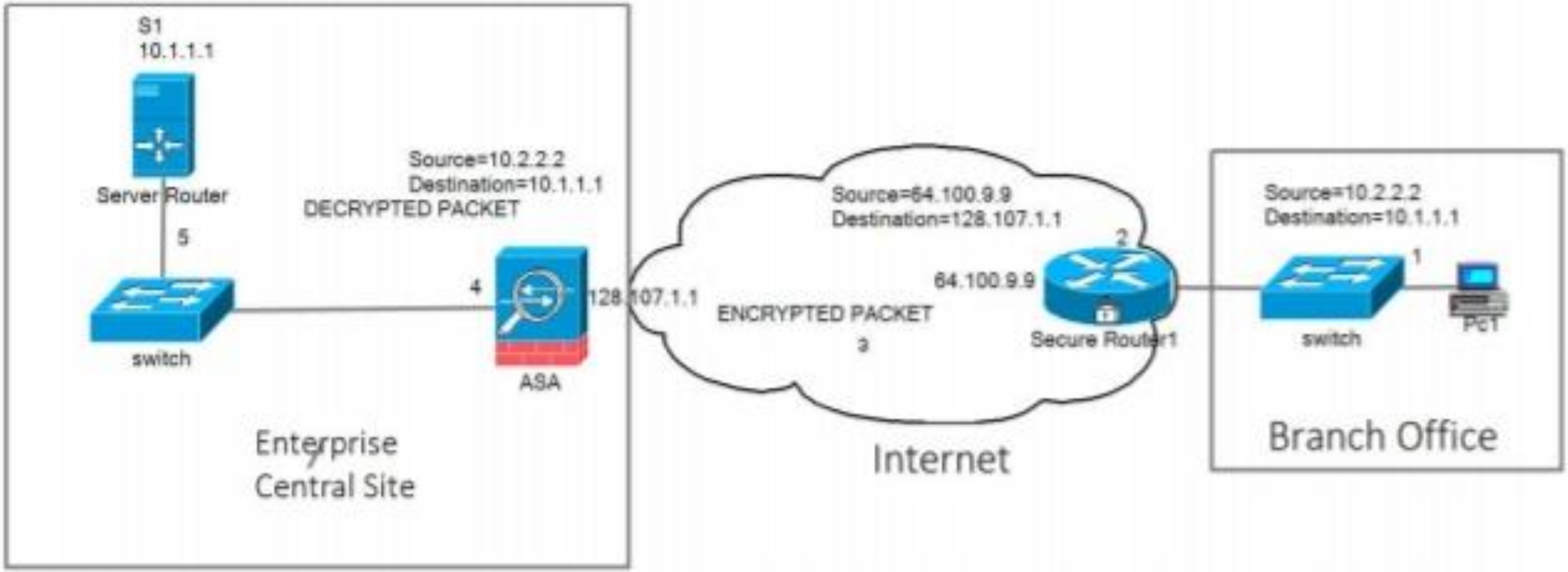
BitDefender total security Kaspersky Total Security and McAfee Live safe are used for users Security purpose.

ASA firewall Software is mainly used for its features as mentioned in the previous slide.

Block Diagram / Architectural Diagram



Block Diagram / Architectural Diagram



VPN TUNNEL CONCEPT FOR A SITE-TO-SITE INTRANET VPN

Dependencies

List all the dependencies in your software :

Benefits of vpn :

1. Confidentiality 2.Data integrity 3.Authentication 4.Antireplay

The goal of Ipsec :

1.Confidentiality Is achieved by encryption method

2. Data integrity 8s achieved by hashing method

3. Pee Authentication is achieved by Preshared keys and RSA digital Signature

4.Antireplay is achieved by applying serial numbers to pockets .

Encryption and Decryption methods:

1.Advanced Encryption Standard (AES)

2. Triple Digital Encryption Standard (3des)

3.Blowfish

4.Digital Encryption Standard (DES)

5. International Data Encryption Algorithm(IDEA)

FIREWALL to modify Ports like FTP,SMTP,UDP,TELNET,TCP,etc…. Scan antivirus ,Threats ,and worms .Keep alert malicious link,URL ,OR SPOOFING MAILS ,OR CODE enter into the users system. End to end authentication allows vpn client . Allow verify website with SSL certification . Ensure updates of antivirus software . Without authority no one can't Be access server and client side After authentication Files must be download or shared.

SOCIAL IMPACT ANALYSIS WITH COVID19

Examine and explain what social impact your project has on COVID-19

SOCIAL IMPACT:

◆ Large users connect internet,so this heavy traffic.

◆Using vpn its speed is minimum because of network traffic nowadays many companies plays huge role through network ,so we can control by configurated setting at server .

◆Avoid using public wifi internet while working with your personal laptop.

◆Most of companies planned to covid-19 to work from home by using office laptop protection level good for their security .

COUNTER MEASURES:

◆During Conference or video conference to provide unique webumar id active 10mins to login at a time.

◆While working at home set screen recording that the user login and till logout it can be uploaded.

◆For firewall authentication mate sure update and turn on notification by connecting mail into your pc.

◆ Turn off your microphone or camera after working and put lock to your pc.

◆ Using personal laptop without scanning or authentication process by headquarter,they should not provide access to that pc.

◆While remote access VPN method high security to configure NAT or access list time configuration time limit for the process.

◆Use paid antivirus and closed server,avoid using free antivirus for security.

◆Email protection by listing method White list and black list.

◆Spam mail destroyed by using email security webserver.

Counter measures :

For further security in VPN, we can use face lock, fingerprint in additional to passwords. Each and every employee should be under monitoring control, which should be updated every minute to the server.

To avoid email attacks, one should install the software in pc or office laptop and connect them with VPN.

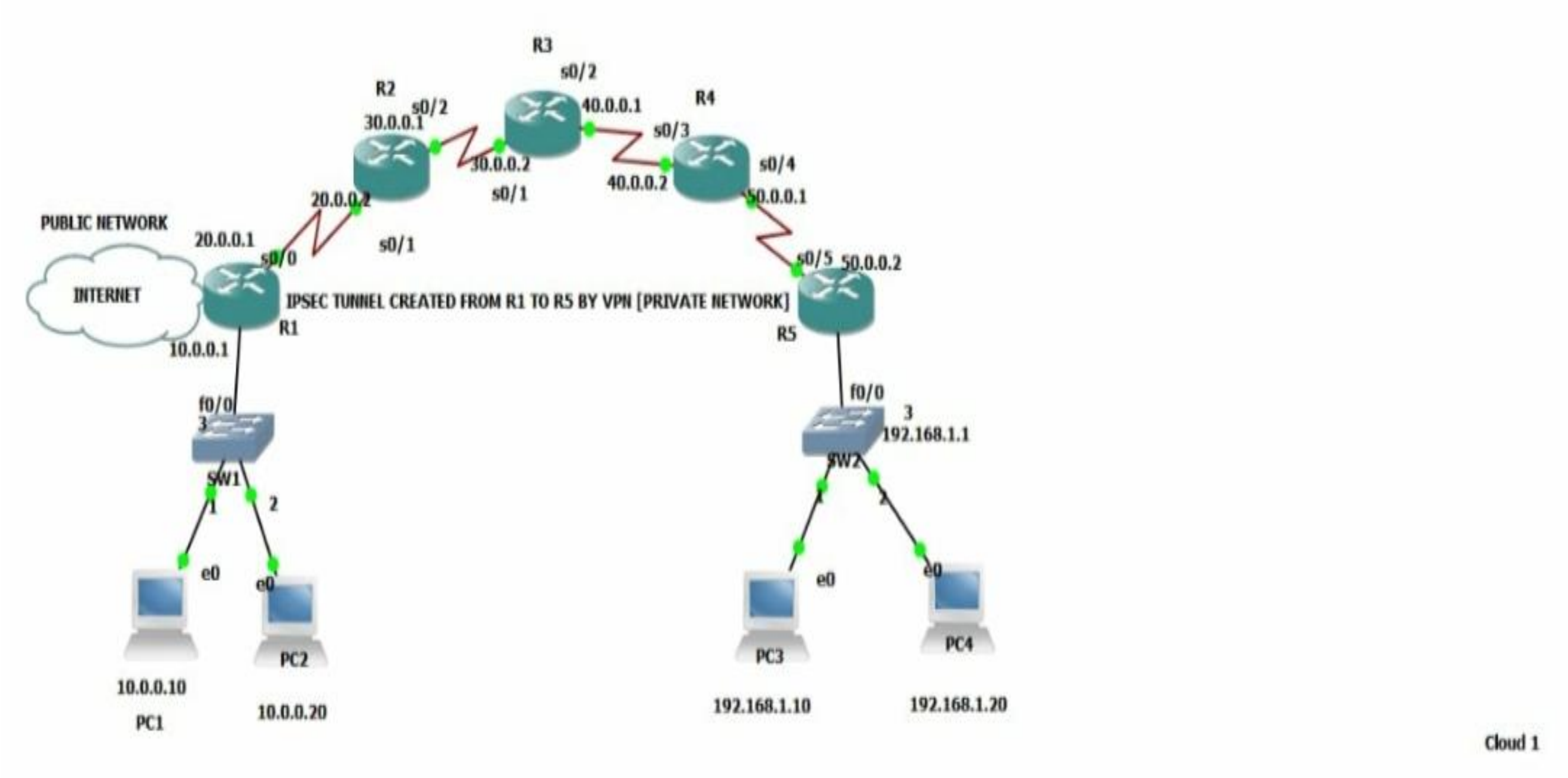
>Go to Whopwnedme
>And enter Your Email
>you can find if someone hacked your email.

- Now ,We End with that VPN concept play big role in covid_19 , because employees via access through VPN login with connect private network overlapped with public network. Most of the attacks by random to controls by high level bandwidth range till 100 gigs depends upon their company network. To avoid attack employees bulids high security and keep updates softwares.

- ***"AS THE WORLD IS INCREASINGLY INTERCONNECTED, EVERYONE SHARES THE RESPONSIBILITY OF SECURING CYBERSPACE"***

Implementation

- Add the snapshots of the project here.



Link to the project

GitHub link:

Google Drive link: