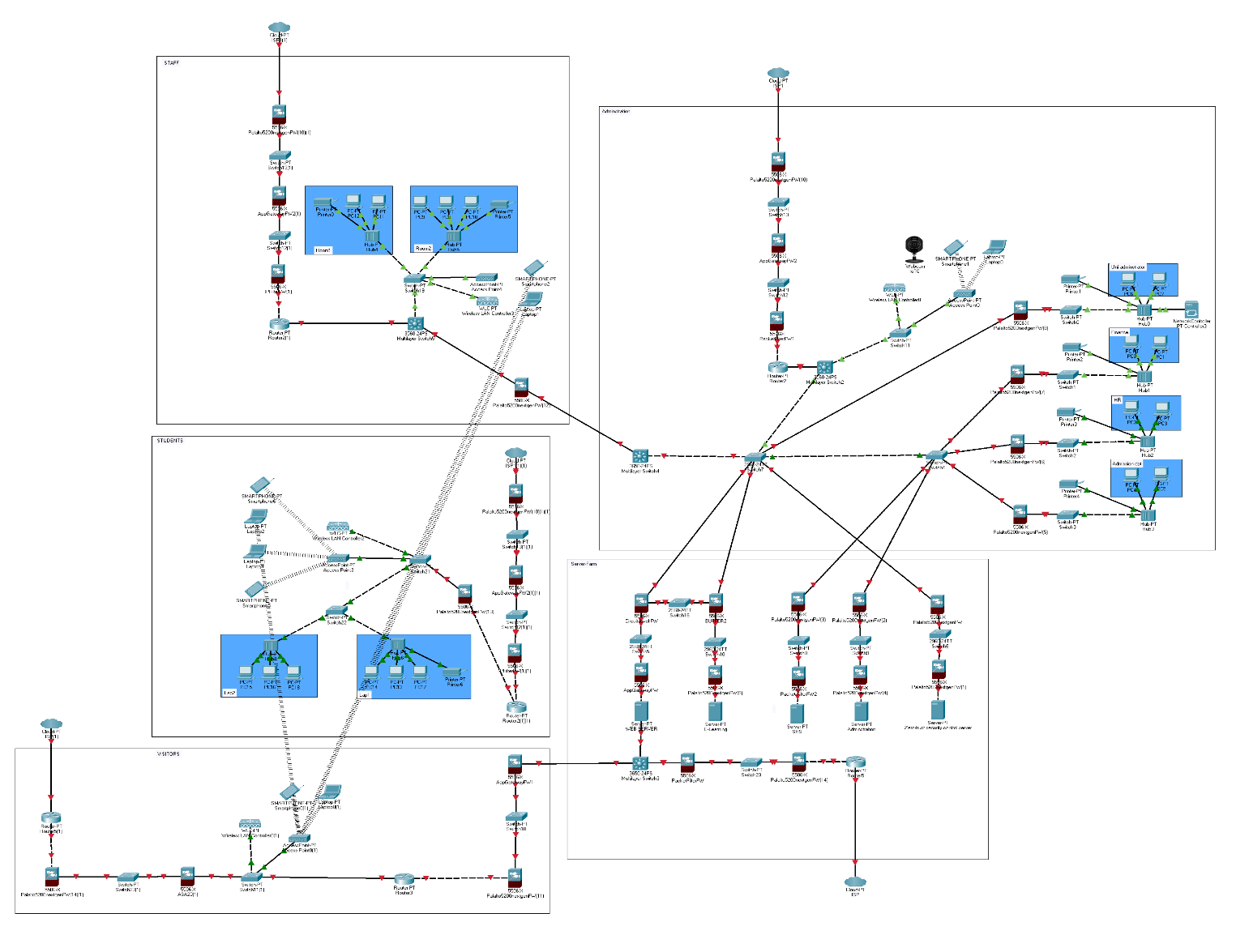


20CSCI34H

Computer System Security

University Network Security

|  |  |
| --- | --- |
| Name | ID |
| Mostafa Ebrahim Negm | 153095 |

Network Architecture: 

Problem definition:

Designing a security system for the British University in Egypt they provide a general solution that suite each group of users at the university. (Administrative Users, Students, Academic Staff, Visitors). With containing each group independency and obtaining that all resources are preserved by the CIA triad. Each group of users has it is own unique privileges and features.

Zero Trust Security Approach:

The Zero trust approach is built on concept of Never Trust, Always Verify. In the cyber and network security industry most of security professional are switching to a “Zero Trust model” which states that No device, user, workload, or system should be trusted by default as every device should be verified before each permission or process regardless their location neither inside nor outside the security perimeter.

Any network consists of 5 components which are (Workloads, Devices, Data, Networks, Users)

And the Users are the weakest point in any network. The zero-trust model adopts a security posture of “Default denial” where the system is isolated until a certain level of trust is established. The zero-trust divided into seven principles. Which will be discussed below.

Zero Trust Networks:

To establish a zero-trust security must realize it works on rule of “Divide and Rule”. The network must identify it is valuable assets and define a “micro segmentation” around these assets to create multiple inspection points the block any threats or malicious activity. So, in case of breach that threat can be easily isolated from the rest of the system.

Zero Trust Workloads:

All the workloads must be secured specially the workloads run on public clouds as they are vulnerable to malicious actors.

Zero Trust DATA:

This principle is applied by protecting the data while it being shared continuously between the Application servers, databases, SaaS applications, mobile device, workstations, cross the whole university and public network.

Zero Trust Users:

With share of 81% of data breaches involving stolen credentials, username and passwords are not enough to prove the identity of the user. And can be easily deceived or compromised. So, the protecting the users’ valuable assets must be strengthened.

Zero Trust Devices:

With share of 70% of breaches include an electronic device that been compromised, eery device connected to the network should be treated as threat vector whether the device is a workstation, mobile device, or IoT/OT device. The device must be able to be isolated by security team in case of breach.

Analytics and Visibility:

The analytics are a very important corner stone at the zero-trust approach as you cannot protect what you cannot see or understand so, the model always monitors the users and device logs, and correlates and analyse every activity on the network. And to achieve the desirable level of security the analytics must be to identify every user activity and his routine or activity pattern on the network to alarm in case of any suspicious activity happens on the network.

Automation:

The zero-trust approach requires automatic IT environment to be able to speed the incident response, policy accuracy and task delegations.

Implementing Zero-Trust:

Most of businesses and organizations has realized the power of zero-trust in preventing cyber-attacks. The zero-trust architecture is also simpler than it looks. As it works as augmentation of the existing architecture. Without adding any addition technologies or modifying the current architecture technology. Rather it can be deployed at the same time with taking advantages of the current technology that the architecture has. As most of the zero-trust implementation is in layer 7. However, most of organizations are still stuck with the traditional security-models with the concept of “Trusted-user, Untrusted-user”. The user can simply move from traditional network into a zero-trust network by only by moving datasets, applications, assets, or services to the zero-trust network without any complications. Which make the zero-trust is manageable, cost-effective and nondisruptive. To implement a zero-trust we are going throw main steps.

1. Define the protect surface.

Implement a zero-trust network requires a good definition of the protected surface which include (Data, Applications, Assets, Services). In current days it is hard to maintain a network security tirelessly with an always expanding surface which makes is more vulnerable to threat landscape. With zero-trust rather than focusing on the macro level attack surface it focusses more on the protect surface. The protect surface composed of (Critical data, Apps, Assets, Services -DAAS-)

DAAS (Desktop as a service): are one of most valuable service should be protected.

As example for the previous protect surface.

* Data: credit card information, Person identifiable and intellectual property.
* Applications: custom software (E-Learning, Admission website).
* Assets: SCADA controls and IOT devices.
* Services: DNS, DHCP and Active Directory.

After defining. We can move them close to the protected surface so we can create a small perimeter with policy that are limited, precise and understandable.

1. Map the flow.

To design the network in correct way, it is important to understand the system flow and how does the system should control the data traffic inside it, especially the data under the protect surface. And t know how it should be protected. This could be accomplished by scanning the network components and how they interact with each other, and how the data transactions work between DAAS with other resources. With gathering all these valuable information, we can now start a Zero-trust architecture and knowing where we should insert controls.

1. Architect a zero-trust network.

Building a zero-trust network is a completely customized as it does not have a universal single design. Instead, it is all designed around the protect surface. After collecting all the previous information, you can now start implementing the network with the next gen of **firewalls:** from “paloalto – PA-5200 Series” as these firewalls works as segmentation gateway creating a micro perimeter around the protect surface. To allow us additional layers of control and inspection all the way to layer 7, for anyone or anything is trying to access the protect surface. These fire walls are the corner stone of the zero-trust approach as they are the world’s first ML-Powered NGFW securing the system from unknown threats. And reduce error by using automatic policy recommendations. The paloalto NGFW classifies all the traffic include applications, threats and content then connect the traffic application the user regardless of the user’s location or device type. As both application and user are the main elements in the system by known each user daily traffic or routine and classifying them will improve the result in security posture and reduce the incident response time. FW that are powered by ML have power to prevent for file=based attacks while identifying and immediately stopping phishing attempts. Also cloud-based ML able to push zero-delay signatures and instructions to NGFW which helps to achieve “Availability”. The NGFW also uses behavioural analysis to be able to recommend policies based on the environment. Also have the future of automating the policy recommendation which saves time and reduce the risk from human error.

Also, able to identify and sort all applications on all ports with full layer 7 inspection. The FW uses the application name for all the policy enablement instead of port for safety and enable safety measure. for allowing, denial, inspection and traffic forming. Also, the ability to create a custom application-ID from the paloalto apps. Also identifying payloads such as files and data pattern to be able to block a malicious threat file. With the ability to create report that include SAAS reports to provide a full vision over the network. And the ability to set application-ID based on rules built within the policy optimizer giving more secure and easier to manager rule.

The ability of enforcing security for users at any location on any device:

Enable security policies, reporting and forensics based on users and groups not just IP address.

Integrates with repositories to leverage user information as (WLAN controllers, VPNs, directory server, proxies and more).

Allow defining a group of users on the firewall to take time-bound action without wating for change to be applied within directories.

Applies consistent policies despite of users’ locations

(Office, home, travel, etc.) and devices (iOS and Android mobile devices, macOS, Windows, Linux desktops, laptops; Citrix and Microsoft VDI and Terminal Servers).

Applying MFA (multi-factor authentication) on the network layer of any app to prevent organization credentials from leaking to third-party websites and prevent reuse to stolen credentials.

The ability to take a dynamic security action based on the user behaviour to restrict and suspicious action or malicious file.

Having the ability to prevent malicious files concealed in encrypted traffic.

Also, the security can be extended with cloud delivered security subscription as:

* Threat prevention: by automatically inspecting all the traffic on the network and block known vulnerabilities, malware, exploits, spyware, command and control, and custom IPS (intrusion prevention system).
* WildFire Malware prevention: using ML protection with cloud-based analysis to prevent any new threats in and discover remediate evasive threats.
* URL filtering: prevent access to malicious websites and protect users against web threats including phishing attacks.
* DNS security: detect and block known and unknown threats over DNS and prevent attackers from bypassing security measures.
* IoT security: discover all the unmanaged devices in the network accurately using ML without deploying sensors, identify the risk and vulnerabilities and prevent known and unknown threats. And advice policy recommendation and automation enforcement.

1. Zero-trust policy:

“Kipling method” is the method we will use to create our zero-trust policy after finishing the architecture. By making a white-list of resources that should have access to users on the network instead of the traditional way “trusted or untrusted”. The Kipling method uses a four-question concept “who, what, when, where why and how” to be able to define certain characteristics.

* + 1. Who: should be accessing the resources?
    2. What: are the apps that being used to access the resources under the protect surface?
    3. When: the resources being accessed?
    4. Where: is the packet destination?
    5. Why: the packet wants to access these resources under the protect surface?
    6. How: is the packet is accessing a certain resource under the protect surface with an app?

With this level of policy enforcement, we can guarantee that only known traffic will be allowed and legit apps have a communication permission.

Kipling method apply:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Who** | **What** | **When** | **Where** | **Why** | **How** | **Action** |
| User-ID | App-ID | Time | System Object | Classification | Content-ID | --------- |
| Finance | Treasuryapp | Working hours | Uni | Toxic | Fin-EID | Allow |
| Staff | Browser | Any | Egy | Toxic | Staff-EID | Allow |

The policies should be created on the segmentation gateways’ the NGFW from paloalto provides this function where should the Kipling method be applied. Also, they help to generate transparent policies to the end user and define what is the APP-ID, Content-ID

How does it will enforce the policy.

1. Monitoring and network maintenance:

At this step all the internal and external logs should be reviewed all the way to layer seven. Focusing operations on the network, inspecting traffic and providing an insight on how we can improve the network over time.

Architecture modelling:

We have in our network five sub-networks which are “Server farm, Administration, Staff, Students, Visitors”. We will start with

* Server farm: in this area we have 5 main servers which are

1. Security server: the one responsible for inspecting and deploy security and policy enforcement apps. Keeping all the logs only can be accessed with employees working with university admin requires a high clearance.
2. Administration server: the one responsible for saving the university administration data that includes information about collages, staff board, and managing software’s, and DAAS as payments only can be accessed from other Administration dept with.
3. SRS server: the one responsible for saving data about the students includes their previous educational experience and their current, faculty, grades that includes TA’s that are part of post-graduate programs.
4. E-Learning: server responsible to save staff E-learning modules, previous exams and laps could be accessed via internal network made for staff and university admin only.
5. Web server: is the server responsible for managing external users and students, where all the public information should be. Includes E-learning website and application, SRS web application, Administration website. Isolated far from the data server that contain a critical data and resource. This server is heavily protected by different FW’s as it is the only server that are opened to the internet and external users and visitors. Also review some sensitive information on SRS webapp and connected to the E-Learning to provide the staff and students the ability to access the E-learning services from home or anywhere. This server has extra 3 types of FW “Circuit level-FW from cisco, App Gateway-FW (Palalto5200), Packet Filter-FW from cisco”.

The server farm is protected with 12 firewalls distributed between the servers in away to create an access point for each server. Creating a large multilayer DMZ’s. and authorization points to guarantee the most confidentiality between servers and their users that vary with many authorities and data from students and external users to the university admin.

* Administration: consist of 4 departments all connected internally with LAN hubs and together throw a disruption switches made from 2 layers between each on them is a firewall to as authorization access point. This network is connected to external ISP network that provides WLAN throw all departments. Only the university administrator is the one that is allowed to access the external network configurations and WLAN controller. This network is connected to IOT device like security cameras that only allowed to university administrator to inspect. Each staff member has him own credentials that allows him to access his job requirements. Most the administration department are allowed to access administration server and SRS, to add and modify files of university, staff, students.
* Staff: consist of multi rooms and offices that are connected internally via LAN network and connected via one-layer disruption switch and core that is connected to the administration department to be able to reach server farm. And of course, a NGFW as authorisation access point, also, connected to external ISP network to provide internet into these offices and rooms. They can connect to the E-learning internal network to upload and modify their teaching modules. Each staff member has his own credentials that belong to him only to allow him to access his course and his files.
* Students: consist of many laps that contains university workstations that are connected in internal network hub and laps connected throw switches. This network is isolated from the internal network between the staff and the administration. For safety purposes. The students can access the university services via internet to the web server at the server’s farm. The student network is connected to the external ISP network. They can access E-Learning, SRS, Administration website only via websites and webapp on the webserver.
* Visitors: they can be considered as internal university visitors or external university website visitors they only have routers and switches that makes them able to connect to ISP external network that route them to the university web server at the server’s farm. They are not connected internally with any of the university network they are only able to see administration website and university main website.

CIA Principles:

With the previous FW and architecture, we could achieve the CIA triad which are Confidentiality, Integrity, Availability.

* Confidentiality: refers to keeping the data private or secret. Been achieved by controlling the access by zero-trust policy and allowing only authorized users only have access to specific assets.
* Integrity: refers to ensuring the data are trusted and correct, authentic and reliable. This be enforced by using firewalls and zero-trust policy that keeps logs of all changes and modification over the network in case. Despite that the only employee who are allowed to modify must authorised at the first place.
* Availability: ensuring that the network users have authorization to access data and application running on the network whenever they need. Been achieved by isolating the data and the control application away from external users in isolated server protected with FW and DMZ. Only allowed to be access with authorized users. Also, will protect the data far away from any security breach happens to the public web server. Also, data can be uploaded on private cloud in case of natural disasters.
* Authentication: using zero-trust policies that requires two-factor authentication to establish a user/session to reduce the risk of stolen credentials or unauthorized access to resources.

Inconclusion all the CIA principles been achieved successfully thanks to the zero-trust technology and policies.

University security policy:

The security policy is a set of rules been added in a clear way to show each user responsibility towards the network and organize conditions and practices to ensure availability and secure network.

At this part we will quote from university of Winchester at UK. As a reference.

“

Policy main goals are:

1. Ensure availability.
2. Protect the Network from unauthorised access.
3. Protect the Network from accidental disruption.
4. Protect confidentiality.
5. Ensure network access can be audited.
6. Define how the network should be used. And what is considered as unacceptable behaviour.

Penalties for breaches of this policy, including potential disciplinary processes.

1. Physical and environmental security device protection

* All the network devices that include” router, switches, cores and control and management systems”, should be housed in secure location with applying all security measures includes a secondary electricity generator “UPS”. And locked with access control system.
  + Entry to the secure network devices area only in case of critical emergency or in case of network device failure. Only allowed to access for authorised employees.
  + Implementing code and card access system and only given to the authorised employees.

4. Access control to the network

* Accessing the network will need a secure login process and accepting a security policy.
  + Registering and removing a user process to be able to access the network will be taken from HR System to be able to create staff/administration access. And for the students and post-graduate students are going to use SRS for their access. There will be a different authorization to help in remote access to the network.
  + User accessing rights on the network is based on user’s job requirement, rather that preference or perceived need.
  + Network administrator rights will be based on requirement of the user job, a list that will securely maintained and reviewed.
  + All the employees and network users should be away for the network policy and agree on it before login into the university network.
  + All users wither staff, administrators or students will have their own unique login credentials.
  + The login credentials should be securely kept without sharing with others.

6. Wired network

* Nothing can be connected to the network except the university owned devices and computers.
  + The university campus, offices and laps are equipped with wireless networks, which can be used to feed personal laptops and mobile phones. Personal devices are not allowed to connect with the wired network in any case. Unless formally request then logged under the supervision of the IT.
  + Any using for the network addresses other than IT provided is not allowed.
  + Accessing network equipment and servers farm is only limited for authorized users.
  + Users cannot connect any wired network physical layer device without agreement from IT.
  + The wired network has been established to service legitimate authorized staff member to support their teaching and research or students lap services.

7. Wireless network

* The campus is equipped with wireless network access points across the campus. Which can be used for users include visitors. This network follows security standards which are:
  + The ITs can provision and monitor the guest SSIDs or user connected to the WLAN network.
  + Any unauthorised device will be blocked from the network without any warning
  + The WLAN will follow WPA2 as it is one of the most preferred Wi-Fi protocols.
  + It is forbidden to connect any wireless network hotspot to the university WLAN.

9. Protection and malicious attacks

* The IT and university admin will ensure to protect the network from:
  + Viruses and malicious software that could threat our network or critical resources under the protect surface.
  + They are allowed to monitor the traffic on the network, network access and intrusion detection system
  + The network will be monitored for potential security breachers or threats under the comply of legislation, and all the activity will be kept in logs.
  + They are allowed to access, modify or delete all data stores on or transmitted across the University’s network. This includes data stored in personal network folders, mailboxes etc.
  + Having the rights to block or disconnect device that is connected via LAN or WLAN network in case of suspicious activity or threating the system.

10. Enforcement

Any user (employee, staff or student) been found violating the policy will be subjected to disciplinary or legal action. Deviation from the policy is allowed in extreme cases and been provided and reviewed by the university admin and leader board and approved on.

Reference:

1. [\*Simplify Zero Trust Implementation Using a Five-Step Methodology (paloaltonetworks.com)](https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/white-papers/simplify-zero-trust-implementation-with-a-five-step-methodology.pdf)
2. <https://duo.com/resources/ebooks/the-2020-duo-trusted-access-report?utm_source=cisco&utm_medium=referral#get-the-report>