|  |  |  |
| --- | --- | --- |
| Qualification Code: | ICT60515 | |
| Qualification Title: | Advanced Diploma of Computer Systems Technology | |
| Unit Code/s: | ICTNWK607 | |
| Unit Title/s: | Design and implement wireless network security | |
| Student Id | Cal14385330 | Date : |
| Student Name | Benjamen Calleja | |
| Assessment Due Date: |  | |
| Assessment Name: | Assessment Item 3, Project | |
| Teacher’s name: | Murad Quazi | |
| Teacher’s email: | mquazi@kangan.edu.au | |

|  |
| --- |
| 1. Task Instructions |

This Assessment Item is project and it requires students to work in team (max 3 students in a team) and address all requirements as per Assessment item Description. Students are required to accomplish their task professionally and in time. Students must submit this Assessment at myKangan. This assessment item is project. It is open book and classroom based. Students are allowed to research on Internet. Allocated time for this assessment item is one hour.

|  |
| --- |
| 1. Submission instructions |

All items submitted must be clearly marked with the following details:

• Your full name

• Your student number

• Your class group

• The date

This cover sheet must accompany all items submitted.

By signing this document the student has read and accepted the Department’s assessment item submission policy as outlined in the ICT Student handbook and that:

1. The content of this assessment or assignment is my/our own work. Where the content is not original acknowledgments have been noted;
2. I/We have made a copy of any electronic, digitally prepared or paper based submissions as proof of completion.

|  |  |  |  |
| --- | --- | --- | --- |
| Student Signature: |  | Submission Date: |  |

# Marking Criteria

|  |  |
| --- | --- |
| **Grade** |  |
| NP | * Assessment aims have not been met |
| P | * All requirements mentioned in Task A and Task B are correctly addressed. * OHS Risks are identified and documented |
| CP | * All requirements mentioned in Task A and Task B are correctly addressed. * OHS Risks are identified and documented * Graphics are accurate and clearly presented * OHS Risk control measure are taken |
| DI | * All requirements mentioned in Task A and Task B are correctly addressed. * Graphics are accurate, well presented and clearly reference if required. * Comparison is done wherever required * OHS Risks are identified and documented * OHS Risk control measure are taken * Proper Documentation is done |
| HD | * All requirements mentioned in Task A and Task B are correctly addressed. * Graphics are accurate, well presented and clearly reference if required. * Comparison is done wherever required * OHS Risks are identified and documented * OHS Risk control measure are taken * Contents are comprehensive, accurate and professionally presented * Requirements are explained with Graphics. * Proper Documentation is done |

|  |  |
| --- | --- |
| Comments: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Teachers Signature: |  | Date: |  |

|  |
| --- |
| 1. Assessment Item Description |

**Students are required to Configuration WLAN for John Pty Ltd and implement all security measures on John Pty Ltd’s network.**

This assessment Item is Project. Students are working as a network specialist for JOHN PTY Ltd. John Pty Ltd is planning to extend their wireless network. They want to implement all security measures on Network. You are required to configure wireless network and implement all required security measures on your Network. This assessment item has two Tasks (Task A and Task B) and students are required to complete both tasks. This project requires students to work in team (max 3 students in a team) and accomplish their task professionally and in time. It is team leader’s responsibility to inform teacher about individual student’s responsibility. Students are required to research their own component. Marking Criteria for this Assessment Item is as per marking criteria.

**Task A: Research Component:**

**Research and explain**

Students are required to research and explain following:

1. Research and list appropriate hardware to meet WLAN and Security requirements  
   **Wireless Access Point Is a device that creates a wireless local area network (WLAN). Access points are essential components of a wireless network’s infrastructure. They provide a wifi signal to a specific area, and are generally used in offices and buildings.**

**On-site and cloud managed WLAN. Most larger wireless network deployments require a WLAN controller or internet hosted wireless network management system to manage the access points. Wireless Lan controllers (WLC) are access point managers that are mounted to a server rack and acts as the brains of the wireless network setup. The controller tells each AP what settings to have at any given time so as not to disrupt the rest of the wireless infrastructure.**

**Network Switch A network switch is a piece of equipment that connects all network devices together. Because they use PoE (Power over Ethernet), new switches act as the power supply for connected devices**

**Power over Ethernet PoE allows a device to receive computer data and power at the same time by sending both over the same Ethernet cable. By using devices That support PoE, the need for electrical power at the exact location of the installed device is eliminated**

**Firewalls help to protect networks from unauthorized access to or from a network. They can be hardware or software based**

**Wifi Enable Device Like internet access, it is necessary to have some kind of device to connect to the wifi once a new network has been implemented. This can be a laptop, smartphone, tablet, or any wifi enabled device.**

1. Research and name at least two available devices for WLAN and explain how they are different  
   **Access Point   
   A wireless access point (AP) allows wireless devices to communicate and are commonly connected to cabled networks to allow wireless users access to the network.  
     
     
   Wireless Bridge  
   Wireless bridges can be used to connect networks together and also extend the range of the network. A WLAN bridge can be used to connect networks up to three miles apart with a Long-Range Wireless Bridge allowing communication to take place up to 25 miles apart**
2. AAA Authentication **AN AAA server is a server program that handles users requests for access to computer resources and, for an enterprise, provides authentication, authorization and accounting (AAA) services. The AAA server typically interacts with network access and gateway servers and with databases and directories containing user information. The current standard by which devices or applications communicate with an AAA server is the RADIUS**
3. Research and explain one of following Guest access services
   1. Anchor  
      **anchor mobility, or guest WLAN mobility, is a key feature of the Cisco Unified Wireless Network solution. It offers the ability to map a provisioned guest WLAN to one or more (anchor) WLCs by using an EoIP tunnel. Auto anchor mobility allows a guest WLAN and all associated guest traffic to be transported transparently across an enterprise network to an anchor controller that resides in the Internet DMZ**
   2. bandwidth limiting  
      **bandwidth limit exceeded means that the amount of bandwidth that was allocated to the hosting plan has been reached. Bandwidth is consumed when data is retrieved from the server and delivered to the end user (outbound traffic) as well as when the end user uploads data to the web server (inbound traffic).**
   3. Redundancy  
      **A redundant server is a server currently running 0 cameras. Upon detecting a server as being down, are redundant server is used to replace the downserver's camera and device processing in its entirety.**
   4. Scaling  
      **A scale up server increases its workload capacity by adding memory and processing power, e.g. building "up" vs. "scale out" or adding server units.**
   5. VLAN-based  
      **is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2). ... VLANs allow networks and devices that must be kept separate to share the same physical cabling without interacting, improving simplicity, security, traffic management, or economy.**
4. IOS and IP networking models  
   **The Open Systems Interconnection model (OSI model) is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to its underlying internal structure and technology. ... The model partitions a communication system into abstraction layers.  
   The hierarchical set of related protocols in a suite t represents all the functionality required to interface the human network with the data network. The 4-layer TCP/IP model is a protocol model because it describes the functions that occur at each layer of protocols within the TCP/IP suite.**
5. Intrusion prevention system (IPS) and IDS security protection  
   **An Intrusion Prevention System (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. Vulnerability exploits usually come in the form of malicious inputs to a target application or service that attackers use to interrupt and gain control of an application or machine.  
   An intrusion detection system (IDS) is a device or**[**software application**](https://en.wikipedia.org/wiki/Software_application)**that monitors a**[**network**](https://en.wikipedia.org/wiki/Computer_network)**or systems for malicious activity or policy violations. Any malicious activity or violation is typically reported either to an administrator or collected centrally using a**[**security information and event management**](https://en.wikipedia.org/wiki/Security_information_and_event_management)**(SIEM) system. A SIEM system combines outputs from multiple sources, and uses**[**alarm filtering**](https://en.wikipedia.org/wiki/Alarm_filtering)**techniques to distinguish malicious activity from false alarms.**

Threat mitigation strategies  
  
**The word mitigation means the act of reducing the severity or seriousness of the impact of something on a situation. IT Threat mitigation is therefore defined as the corrective actions, prevention or remedies put in place to combat or reduce IT threats on a computer, server or network. 'IT threats' is a very broad term that envelops physical, software, and hardware threats that any IT system may encounter.**

Current regulations, standards and certifications in relation to wireless  
***Wireless networking is becoming increasingly important to businesses, both small and large. Use this chart to make sense out of all the wireless local-area network standards.***

**Use this wireless networking standards chart to get quick information to help you differentiate between the available wireless networking standards and choose which standard might be the right fit for your business. See the links below the chart for further information on wireless networking standards.**

1. Explain deployment schemes network topologies, architectures and elements  
   **A network topology is the arrangement of**[**nodes**](https://searchnetworking.techtarget.com/definition/node)**-- usually**[**switches**](https://searchnetworking.techtarget.com/definition/switch)**,**[**routers**](https://searchnetworking.techtarget.com/definition/router)**, or software switch/router features -- and connections in a network, often represented as a graph.  The topology of the network, and the relative locations of the source and destination of traffic flows on the network, determine the optimum path for each flow and the extent to which redundant options for routing exist in the event of a failure. There are two ways of defining network geometry: the physical topology and the logical (or signal) topology.**

**Architecture must consider bits and pieces of topology when it comes to design. Essentially from what I’ e gathered about topology it's essentially studying objects under continuous deformation, without leading to destruction. So stretching or bending, but not breaking or tearing.**

**How does this apply to architecture though? Until very recently most architects didn't care much for studies such as topology. They considered it a interment(I may have made that word up) to the growth of design. However, the recent evolution of modern design has not only encouraged research in such fields.**

Research and produce security solutions plan  
The following six elements of strategic planning are the keys to successful strategic planning:

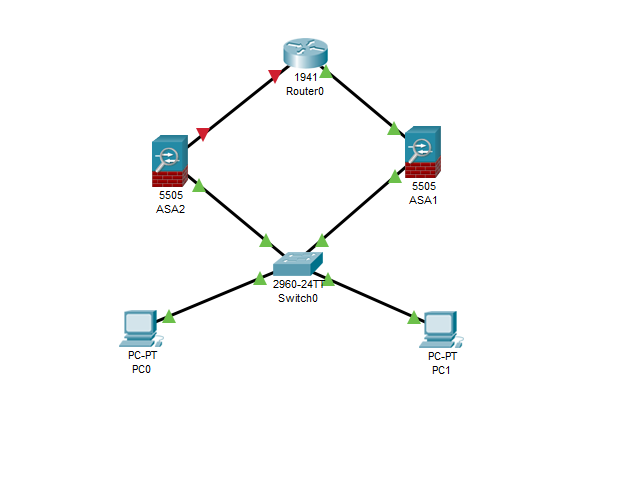
1. Simplicity
2. Passion (emotional energy)/Speed of Planning and Adapting
3. Connection to Core Values
4. Core Competencies
5. Communication
6. Implementation  
     
   **Simplicity**  
   Regardless of the methodology and tools employed, a strategic direction must be simple enough to be understood by not only the strategic planning committee, but every stakeholder in an organization. One good metric for assessing the clarity of your strategy is an "elevator speech." An elevator speech is a 60-second summary of your strategy that presents a compelling overview of strategic direction. The speech should be short, easily understood, and motivating.  
     
   **Passion (Emotional Energy) and Speed of Planning and Adapting**  
   If a strategic direction has no emotional connection for those who are charged with moving, implementing, selling, telling, living, breathing, and executing the strategy, the strategic direction is DOA. Strategic planning is a marathon, not a sprint. It takes emotional stamina for an organization to move toward a vision. It takes speed and passion to win in today's environment: speed to get good data from the frontlines of an organization into the planning process; speed to analyze the data; speed to react to it; and speed to move in an altered direction when necessary. Once a year planning cycles for strategic planning are DEAD; they are too slow, too ponderous, and too removed from today's business cycles. Current practices spend too much time looking at the past to predict future trends or trying to explain what went wrong in previous planning cycles. Many tend to focus on year-long market research cycles, big glossy pictures, and graphs instead of considering inputs that will drive the organization into the future.  
     
   **Connection to Core Values**  
   Core values are the emotional engine that drives people and organizations forward. Being explicit about a strategic direction and how it links to the organization's core values and competencies helps everyone understand why the energy, focus, and costs are worth it. Values are the "how" an organization expects to conduct business. Values that are understood, communicated, and made part of an organization's vision help guide the daily activities of those who work within that organization. When people understand the values that are at the heart of an organization, they have a better understanding of how to move toward realization of that vision.  
     
   **Core Competencies**  
   Core competencies are the specific, extraordinary abilities that give your organization an edge in the marketplace, service sector, or the like, and cannot be easily imitated. They deliver value to customers in the form of technical expertise, customer and supplier relationship, product development, organizational culture and/or employee involvement. C. developed the main ideas about core competencies in both their series of *Harvard Business Review* articles and their follow-on best-selling book *Competing for the Future.***Communication**  
   A strategic plan must be communicated in multiple ways to multiple stakeholders. Secrecy about strategic plans hamstrings organizations through lack of understanding, absence of ownership, and insufficient input. Strategic plans have to be communicated, and a dialogue of rich information must be continued throughout the planning and implementation phases. No strategy remains static; daily events provide a constant flow of information to be reviewed.  
     
   **Implementation**  
   A good strategic plan means nothing without implementation. Having a clear implementation plan is crucial to successful strategy. Integration is key to the successful implementation of strategic initiatives and objectives. Your implementation plan must be linked to those initiatives and objectives. Implementation is the enacting plan to integrate security into the organizational system and often extend it into the supply chain as well. Integration is sometime referred to as security convergence. *Security convergence* refers both to the threat side and the solutions side of security. It takes a sophisticated holistic (systems) model to understand and plan for integration.
7. Research and list two network tools to test Wireless Network  
    **MetaGeek InSSIder is a WI-FI connection troubleshooting tool that can use to figure out why your WI-FI is dropping and what’s behind your network connection issues. It gives you an overview of nearby wireless networks, SSIDs, as well as channel information, and can also come in handy for locating rouge Aps. It used to be available as a free version**

**The netspot tool is a free Wi-Fi survey app that you can use to scan your network, locate signal leakages, create Wi-Fi heatmaps and create in-depth site surveys.**

1. Analyse firewall solutions for the WLAN **A firewall is a device or piece of software that controls what data is allowed to pass through it. You can use a firewall in a network to separate all the wireless data traffic from your wired network. It is important to understand that no single solution will give you a guaranteed protection against existing WLAN vulnerabilities. In most cases, the best way to secure your network is to:**

**set up and maintain the network and the connected devices correctly.  
implement appropriate safety measures.  
Train your staff on acceptable use and networking best practices.**

1. Create Design for Network and submit for the approval.



1. Research and explain following:
   1. anomalous behaviour attacks  
      **anomalous behaviour attacks is an intrusion detection system for detecting both network and computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous. The classification is based on rules, rather than patterns or signatures, and attempts to detect any type of misuse that falls out of normal system operation. This is opposed to signature-based systems, which can only detect attacks for which a signature has**
   2. client misconfiguration  
      **Client misconfiguration is simply defined as failing to implement all security controls for a server or web applications, or implementing the security controls,  
      but doing so with errors. Client misconfiguration can happen at any level of an application stack,**  
        
      denial of service (DoS)  
      **A Dos is an attack meant to shut down a machine or network, making it inaccessible to its intended user. Denial of service attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. Victims of a DoS attacks often target web servers of high profile organizations such as banking**
   3. eavesdropping  
      **Eavesdropping or sniffing attacks is an incursion where someone tries to steal information that computers, smartphones, or other devices transmit over a network. An eavesdropping attack takes advantage of unsecured network communications in order to access the data being sent and recived. Eavesdropping attacks are difficult to detect because they do not cause network transmissions to appear to be operating abnormally.**
   4. Hijacking **Hijacking is a type of network security attack in which the attacker takes control of a communication. In one type of hijacking (also known as a man in the middle attack), the perpetrator takes control of an established connection whie it is in progress. The attacker intercepts messages in a public key exchange and then retransmits them. Another from of hijacking is browser hijacking , in which a user is taken to a different than the one the user requested. There are two different types of domain name system (DNS) hijacking. In one, the attacker gains access to DNS records on a server and modifies them so that request for the genuine web page**
   5. radio frequency (RF) jamming  
      **Radio jamming is the deliberate transmission of radio signals that disrupts communications by decreasing the signal to noise ratio. Unintentional jamming occurs when an operator transmits on a used frequency without checking, equipment generating radio noise.**
   6. signature attacks  
      **Signature attacks vary quite differently from other attacks**

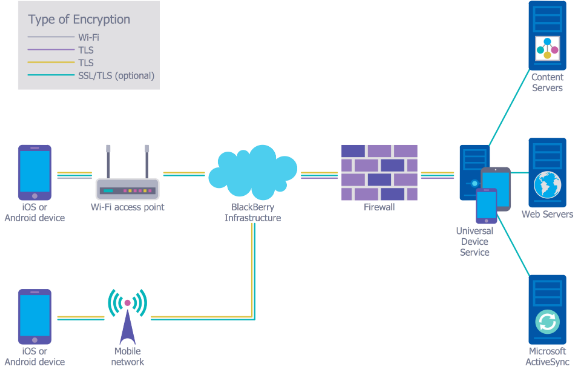
**A file containing a data sequence used to identify an attack on the network, typically using an operating system or application vulnerability. Such signatures are used by an Intrusion Detection System (IDS) or firewall to flag malicious activity directed at the system.**

* 1. social engineering  
     **Social engineering is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.**
  2. access control list (ACL)  
     **File system ACL is a data structure that holds entries that specify individual user or group rights to system objects such as processes, files and programs. These entries are referred to as access control entities. Each system object is associated with a security attribute that identifies its access control list.**
  3. demilitarised zone (DMZ)  
     **In computer networks, a DMZ (demilitarized zone), also sometimes known as a perimeter network or a screened**[***subnetwork***](https://searchnetworking.techtarget.com/definition/subnet)**, is a physical or logical subnet that separates an internal**[**local area network**](https://searchnetworking.techtarget.com/definition/local-area-network-LAN)**(LAN) from other untrusted networks, usually the internet. External-facing servers, resources and services are located in the DMZ. So, they are accessible from the internet, but the rest of the internal LAN remains unreachable. This provides an additional layer of security to the LAN as it restricts the ability of hackers to directly access internal servers and data via the internet.**

**Task B: Configure WLAN and Implement all Security measure on WLAN**

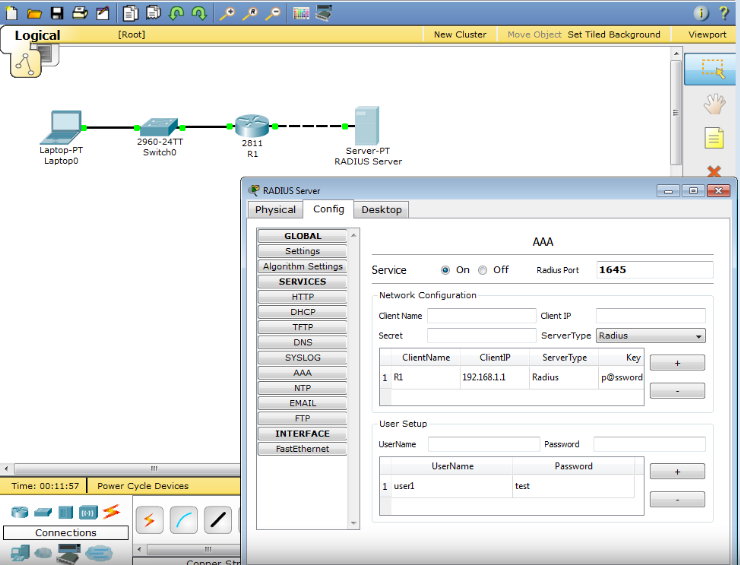
1. Upgrading WLAN of John Pty Ltd to meet the new security threats

To meet new security threats, WLAN should be upgraded by integrating properly hardened and configured network security devices in the infra. These include firewalls, IPS and IDS which make the environment strong and secure.

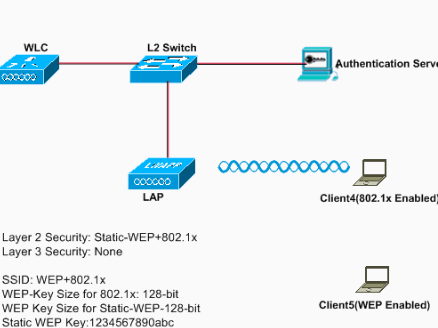


1. You are required to implement AAA authentication (please explain where you are planning to implement AAA authentication)

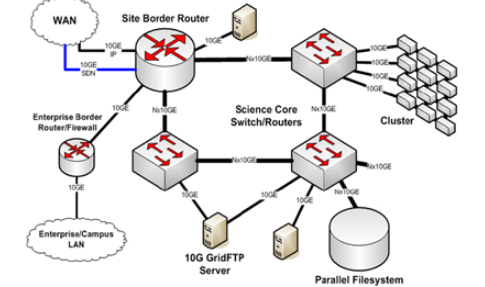
AAA will be implemented in WLAN for the authentication between the machines so that data can travel to the right machine.



1. Clients need to be authenticated using 802.1x method in the WLAN

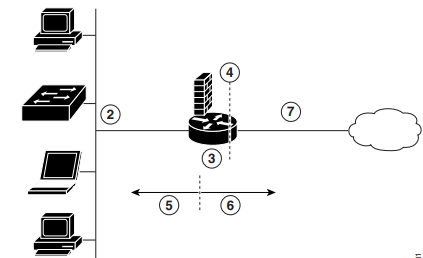


1. Implement your approved network design (Network design created under Task A) and create the network.

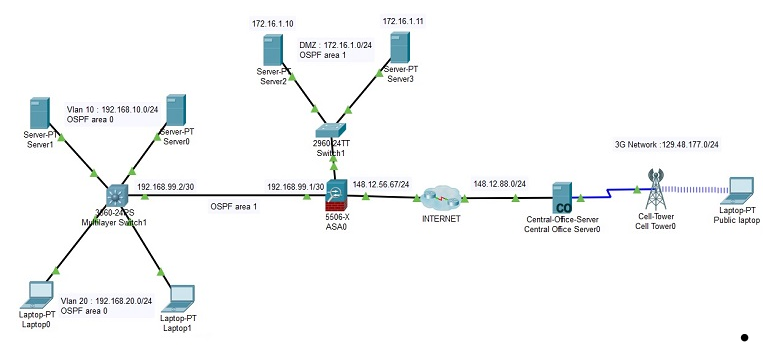


1. Implement firewall for the WLAN

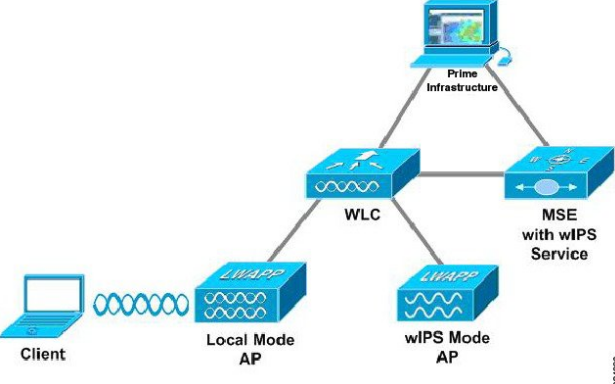
This is the general architecture of how firewall is deployed in the infra:



This the packet tracer configuration of firewall:



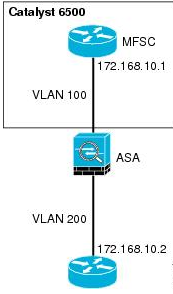
1. Implement the best suitable IDS/IPS in your Infrastructure

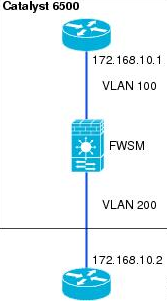


This is the representation of the intrusion detection system or intrusion prevention system that saves the infra from foreign cyber attacks.

1. Configure access control servers for integration with wireless network

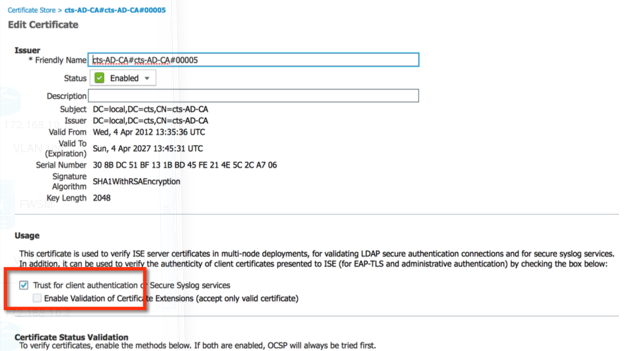
Access control lists can be configured by integrating the firewall devices with the other devices. This configure the network in such a way that it will allow only those IP addresses to go through it which are in the ACL rules.

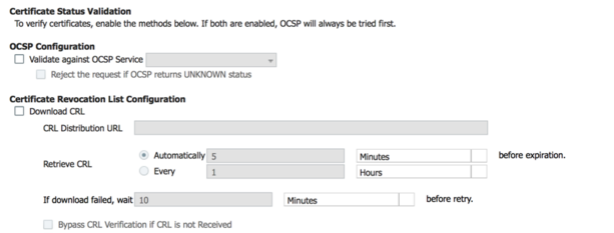




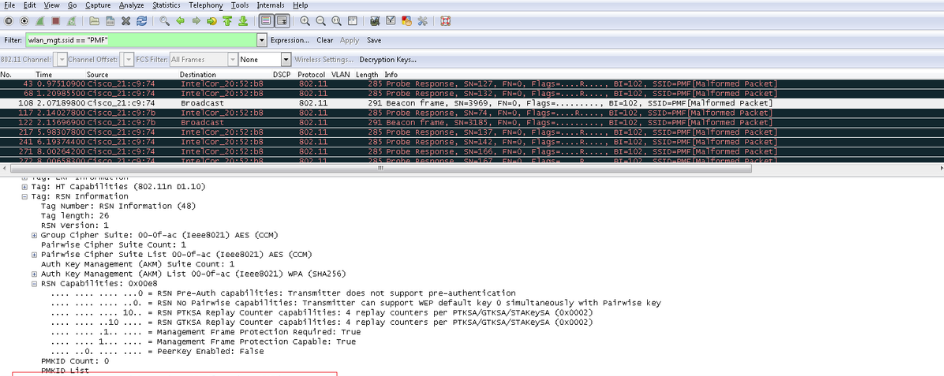
1. Configure client and server-side digital certificate services

Digital certificate is the authentic entity that maintains the integrity of the data between client and server machines. Its configuration is shown below:





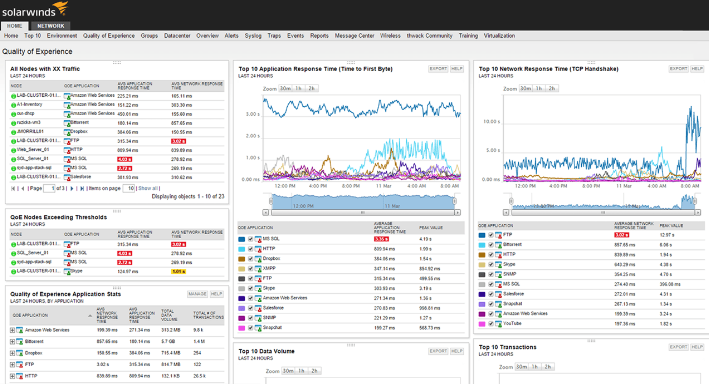
1. Design and configure authentication of clients and management frame protection on clients and controllers



This is the screenshot for the configuration of frame protection.

1. Troubleshoot secure wireless connectivity services

To prevent the issues attacking the security of the wireless connectivity services is keen monitoring of the system. This could be done by the network OPS manager.



1. Troubleshoot integration issues of network with access control

When the infra is properly implemented, there are also tools that are deployed with it so that if in case some outage is about to occur which can help in taking the proactive approach making the outage less destructive and serious. Whenever troubleshooting the network security issue, make sure that there is no loop hole lest and we get to know the root cause of the issue.

REFERENCES:

Čabarkapa, D. (2015). Application of Cisco Packet Tracer 6.2 in teaching of advanced computer networks. *INFORMATION TECHNOLOGY AND DEVELOPMENT OF EDUCATION ITRO 2015*, 153.

Wool, A. (2001, August). Architecting the Lumeta Firewall Analyzer. In *USENIX Security Symposium* (pp. 85-97).

Javid, S. R. (2014). Role of packet tracer in learning computer networks. *International Journal of Advanced Research in Computer and Communication Engineering*, *3*(5), 6508-6511.

Al-Rawi, A., & Lansari, A. (2007). Effect of Windows XP Firewall on Network Simulation and Testing. *Issues in Informing Science & Information Technology*, *4*.

Bassey, D. E., Ogbulezie, J. C., & Effiom, E. O. (2016). Local Area Network (LAN) Mock-up and the Prevention of Cybernetics Related Crimes in Nigermills Company using Firewall Security Device. *International Journal of Scientific & Engineering Research*, *7*(3), 1124-1130.

**Moderation/Validation table**

|  |  |
| --- | --- |
| Assessment Item Number | 3 |
| Version Number | 3 |
| Date Created/Improved | 28/04/2016 |
| Created/Improved by | Murad Quazi |
| Date Validated | 28/04/2016 |
| Validation Team Member | Vikram Behal |