PROJECT 2: Firewall Selection and Scenario of Placement

VOORE. MANI SAI

Computer Networks/ Cyber security

PROF. Merrick Martin

February 18,2023

**Firewall Selection and placement**

1. Firewall for the Corporation Tech Network I selected a Fortinet FortiGate Firewall. The reason behind is which cover areas like Network, Server, and Workstation. The best part about the FortiGate is provide advance security features and can be managed from single source.
   1. The FortiGate Firewall uses a threat intelligence and machine learning algorithms which detect, prevents and provide range of security features – IDS/IPS, Web Filtering, VPN and Malware protection also has a user-friendly interface can easy to manage and configure. The Firewall need to place at the Network perimeter for protection of entire network. In addition, firewall offers VPN functionality allows for the secure connection remotely via network. It also provide the control over the administrator set policies, network traffic it also has web filtering capabilities allows to block data. Fire wall malware protection is the mechanism where it uses sandboxing and behavior analyzer which identifies neutralized potential threats.
   2. When it comes to server and workstation provides the FortiGate has an additional layer of protection against local vulnerability and provide end point protection which includes firewall, antivirus, VPN. This can be done if we enable on all server and workstations.
2. Creating a DMZ Plan: To access the internal resources we need to create a buffer zone among the internal and external network which prevent direct/indirect access to network. This can be achieved by placing in between network and server firewall. We need to restrict only for the common services such as web, email and DNS servers. It is also called a security key component is because which prevents unauthorized access to network. We also need to isolate the traffic flow from external network and public servers. For creating a DMZ, we need to follow steps:
   1. Identify the server and services which are exposed to public.
   2. Design a DMZ topology and also including placement of firewall.
   3. Next is to configure the firewall which allows the traffic flow to DMZ from network.
   4. At last, Deploying a server in the DMZ and configuring them.
3. Plan for the Secure Network Authentication: For the secure network we need to set up a multi-factor authentication (MFA) for all the users who are accessing the network resources. In MFA we are including few protocols like smart card, tokens, digital signature, biometrics, OTP, Captcha etc. To regulate the regular password into more complex password by authentication mechanisms which can greatly enhance the security of networks. To achieve a high-level secure authentication can be done by:
   1. Implementing MFA to reduce the password attacks.
   2. Developing the authentication protocol like SAML and Kerberos.
   3. Monitoring and Auditing logs to detect and prevent attempts.
   4. Regularly updating the password policies and having a best practice on password management.

Graphical user interface, diagram

Description automatically generated

1. Draft Report:
   1. Introduction: As the senior network architect of corporation techs recommends to design a DMZ to increase the network perimeter security and replace a current username and password approach. So for that Fortinet FortiGate firewall is a best solution for organizations. This report provide the Fortinet FortiGate firewall, why it is the best choice for Corporation Techs and where it should be placed to get maximum effectiveness. And also describing a plan for creating a DMZ and how to make secure network.
   2. Overview: The FortiGate firewall uses built hardware and software to provide the advance security network capabilities. This is design in a such a way that it helps to small and large enterprises for their data center, cloud environment platform and branch offices. The FortiGate has it only platform interface where we can configure and manage also set the security policies across the network also for the DMZ.
   3. Features and Capabilities’:
      1. Firewall: It uses the advance traffic packet filtering based on the source, destination, port, and protocols for the organization. Also has the web filtering concept which block accessing to inappropriate websites.
      2. Application Control: The firewall provides a feature to organization for controlling and managing access to specific applications.
      3. Virtual Private Network: The FortiGate provides a secure remote access to network over internet.
      4. Intrusion Prevention: The firewall is integrated with intrusion prevention systems provides protection against threats over network.
      5. Cloud Security: FortiGate provides the visibility and control over the application and data which reduces the workloads for the cloud environment like public, private cloud.
      6. Antivirus: It offers the ability to scan the real time traffic to protect from the malicious codes.
      7. Security Automation : It is a tool where it reduces the burden to the organization because it develop in such a way that it can configure, detects and responds to security threats also provide policies across the network.
      8. SD-WAN: which enable traffic routing optimization can improve the cost and application performance.
   4. Placement for Maximum Effectiveness: For appropriate level of security and filtering packets for passing through network we need to locate at network perimeter, within DMZ, and among the network segments to provide the maximum performance efficiency in a network. It should place in position where data and branch office center to control and inspect in a traffic where it motive is to reduce the security workloads.
   5. DMZ Plan and Benefits: It provide a several benefits like
      1. Threat protection against external network: This can be achieved by placing DMZ in between the traffic flow and allows only authorized users.
      2. Segmentation: This is used at the surface layer for ensuring the packets travelling among the end points which are authorized thus reduce the impact of data loss.
      3. Monitoring and reporting: Which helps in the active directories to find potential threats and provide the detail report on measures to mitigate them.
      4. The key advantage of this firewall is provide the security across multiple user environments also network.
   6. Secure Authentication Plan: It provide various options for authentication like:
      1. Strong policy password: In policy it includes the length, expiration and complexity which makes user credentials strong and difficult to crack.
      2. Multi factor authentication: which combines two or more mechanism which makes password security policy strong and have a extra layer of security to data. Two or more mechanisms like adding LDAP, RADIUS, SAML authentication to ensure authorize user can access the internet.
   7. Network Authentication: In addition to MFA, we need have a best practice on network authentication:
      1. Implementing the single sign on which reduces the password theft and simplify for login process.
      2. By sing certificate-based authentication which make end points secure by providing the thrust among them and allow access to network.
      3. Enforcing user to change password on regular basis can be done by change in security policies.
   8. Comparison with other firewall:
      1. Protection: The Fortinet FortiGate firewall has comprehensive mechanism where it includes botnets, zero-day exploits and malware.
      2. Visibility: In a network which monitor the traffic and enables teams to identify and block threats.
      3. It also provides the advance threats and give a solution to protect from that in a network.
      4. In terms of cost which is effective solution because the design and solution meets the need of every organization irrespective of size including physical, cloud based, virtual appliance also has different deployments tools. In other words it is very flexible to use.

Conclusion: The FortiGate firewall provide a centralized and reporting management capabilities which make easy to manage security policies for the small to large enterprise. It is a suitable choice for organizations because it is known as next generation firewall solution. It is a excellent choice for Corporation Techs network to use this because it has a comprehensive security for networks. The DMZ should be planned strategically a place in a network in such a way that maximizes effectiveness. The FortiGate has several advantages over other firewall for a organization this will be a excellence choice.

# References

*Authentication*. (2023, 02 16). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Authentication

*DMZ (computing)*. (2023, 01 27). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/DMZ\_(computing)

*Getting started: Cookbook*. (n.d.). Retrieved from FortiGate / FortiOS 6.2.0: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/940340/where-to-place-the-fortigate-on-the-network

*Multi-factor-authentication*. (2023, 02 17). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Multi-factor\_authentication

*Next Generation Firewall (NGFW) - See Top Products*. (n.d.). Retrieved from Fortinet: https://www.fortinet.com/products/next-generation-firewall