**EQUIPMENT TEST PLAN**

**pfSense - Windows 2022 AD Server**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Project Title: | **AWS CyberShift Initiative** |  | Date Prepared: | 23rd of June, 2023 |

|  |
| --- |
| **Overall project scope and objectives** |
| The AWS CyberShift Initiative project will secure OzCazual's cloud infrastructure and enable a safe and secure migration from their existing local server to Amazon AWS.  The primary goal is to address the sudden 200% increase in online sales and staff, create a scalable infrastructure that can meet future business demands, and ensure the confidentiality, integrity, and availability of the systems and customer data.  The project will Implementing various security controls, and upgrade the systems and tools currently used at OzCazual |
| **Test objectives and success criteria** |
| Test Objectives:  1. Verify the successful deployment of pfSense as a cloud-based virtual machine, ensuring its compatibility and seamless integration with the chosen cloud platform (e.g., AWS, Azure, Google Cloud). 2. Validate the functionality and performance of pfSense as a network security solution in conjunction with a Windows 2022 Active Directory (AD) Server environment. 3. Evaluate the effectiveness of pfSense in securing network traffic, including firewall rule configuration, NAT setup, VPN connectivity, and traffic monitoring capabilities. 4. Assess the scalability of pfSense in the cloud environment, considering factors such as increased network traffic, the number of users, and resource utilization. 5. Test the failover and high availability capabilities of pfSense in the cloud, ensuring uninterrupted network security and availability in the event of a failure or maintenance activity. 6. Validate the interoperability of pfSense with other cloud-based services, such as load balancers, DNS services, or cloud storage, to ensure seamless integration and functionality. 7. Evaluate the logging and reporting capabilities of pfSense, ensuring that logs are generated accurately, and relevant information is available for monitoring, troubleshooting, and compliance purposes. 8. Test the resilience of pfSense against common network attacks, such as Denial of Service (DoS) attacks, port scans, and intrusion attempts, to verify its effectiveness in detecting and mitigating threats. 9. Assess the ease of management and configuration of pfSense in the cloud environment, including features such as remote access, web-based administration, and automation capabilities.    Success Criteria:  1. Successful deployment of pfSense as a cloud-based virtual machine, without any compatibility issues or errors during the setup process. 2. Verification of essential pfSense features, including firewall rules, NAT configuration, VPN connectivity, and traffic monitoring, in conjunction with the Windows 2022 AD Server. 3. Adequate performance of pfSense in terms of throughput, latency, and resource utilization, meeting the requirements of the intended network environment. 4. Effective network security provided by pfSense, ensuring that unauthorized access attempts are blocked, and network traffic is filtered according to defined rules and policies. 5. Scalability of pfSense in the cloud environment, with the ability to handle increased network traffic, additional users, and resource demands, without compromising performance or stability. 6. Seamless integration of pfSense with other cloud-based services, such as load balancers, DNS services, or cloud storage, without any compatibility issues or disruptions to functionality. 7. Reliable failover and high availability capabilities of pfSense, ensuring uninterrupted network security and availability during failure or maintenance scenarios. 8. Accurate logging and reporting of network activities by pfSense, providing valuable information for monitoring, troubleshooting, and compliance purposes. 9. Effective detection and mitigation of common network attacks by pfSense, ensuring the network remains protected and secure.   User-friendly management and configuration of pfSense in the cloud environment, with features such as remote access, web-based administration, and automation capabilities that simplify the management process.   |  | | --- | | **Test resources required (people, hardware, software, test tools)** |   **People:**   * **Project Manager** : Responsible for overall test planning, coordination, and management of the test activities. * **Cyber Security Specialist**: Responsible for executing the test cases, documenting results, and troubleshooting issues. * **Network Administrator**: Knowledgeable in network configurations and responsible for setting up the virtual network environment. * **System Administrator**: Familiar with the Azure platform and responsible for provisioning and managing the virtual machine on Azure. * **Security Analyst**: Knowledgeable in network security and responsible for testing the effectiveness of pfSense as a network security solution. * **Test Tools Specialist**: Familiar with various testing tools and responsible for selecting, configuring, and managing the test tools used during the testing process.   **Hardware**:  **Virtual Machine on Azure**: Provision a virtual machine running Windows Server 2022 AD Server as the test environment.  **Sufficient compute resources**: Ensure that the virtual machine has adequate CPU, memory, and storage resources to run pfSense and accommodate the expected network traffic.  **Software**:   * **pfSense**: Install and configure pfSense as a virtual machine on the Azure virtual machine. * **Windows Server 2022 AD Server**: Set up and configure the AD Server on the virtual machine to test the integration with pfSense. * **Hyper-V Manager**: Utilize Hyper-V Manager to manage the virtual machine and virtual network settings.   **Testing Tools**:  Select and configure testing tools based on the specific test objectives, such as:   * **Network traffic generator**: To simulate different network traffic scenarios and assess the performance of pfSense. * **Network monitoring and analysis tool**: To capture and analyze network traffic passing through pfSense for security and performance evaluation. * **Vulnerability scanner**: To test the effectiveness of pfSense in detecting and mitigating common network vulnerabilities. * **Load testing tool**: To evaluate the scalability and performance of pfSense under high network traffic conditions. * **Logging and reporting tools**: To capture and analyze logs generated by pfSense for monitoring, troubleshooting, and compliance purposes.  Table - People, Roles, and Time Allocation  |  |  |  | | --- | --- | --- | | **Role** | **Name** | **Resource Allocation** | | **Project Manager** | Giuseppe Raciti | Full-time during test planning and execution | | **Cyber Security Specialist** | Shaun Heywood | As needed, full-time during test execution | | **Cloud Architect / Engineer** | Mark Byrne | As needed, for setting up the virtual network environment. | | **System Administrator** | Mauricio Guerra | As needed, for provisioning and managing the virtual machine on Azure. | | **Cyber Security Specialist** | Shaun Heywood | As needed, for testing the effectiveness of pfSense as a network security solution. | |
| **Test schedule** |
| The test schedule serves as a roadmap for the testing activities involved in evaluating pfSense, a network security solution, in a cloud-based virtual machine environment with Windows 2022 AD Server. It outlines the key milestones, dates, and resource allocations for each phase of the testing process.  The purpose of the test schedule is to provide a structured approach to effectively plan, execute, and report the test activities. It helps ensure that the necessary resources, such as personnel and hardware, are allocated appropriately throughout the testing process. The schedule also helps in managing timelines, dependencies, and milestones, enabling efficient coordination and communication among team members involved in the testing effort.  By following the test schedule, the team can systematically work through different phases, including test planning, environment setup, test execution, and reporting. This approach ensures that all essential aspects of the evaluation, such as performance, security, scalability, and interoperability, are adequately tested and documented. The test schedule helps maintain visibility into the progress of the testing effort and facilitates timely reporting of results, enabling informed decision-making and ultimately ensuring the reliability and effectiveness of pfSense in the specified cloud-based environment.  **Test Schedule**   |  |  |  | | --- | --- | --- | | **Date** | **Milestones** | **Resource Allocation** | | **19/06/23** | **Test Planning** | Project Manager, Cyber Security Specialist | |  | - Define test objectives | Project Manager, Stakeholders | |  | - Identify test resources | Project Manager, System Administrator | |  | - Define test environment | Project Manager, Server Administrator | |  | - Develop test plan | Project Manager, Cyber Security Specialist | | **25/06/23** | **Test Environment Setup** | System Administrator, Cyber Security Specialist | |  | - Install Windows AD | System Administrator | |  | - Deploy pfSense VM | System Administrator, Cyber Security Specialist | | **26/06/23** | **Test Execution** | Cyber Security Specialist | |  | - Test Case Execution | Cyber Security Specialist, Testing Tools Specialist | |  | - Performance Testing | Cyber Security Specialist, Testing Tools Specialist | |  | - Security Testing | Cyber Security Specialist, Server Administrator | | **30/06/23** | **Test Reporting** | Cyber Security Specialist, Project Manager | |  | - Results Compilation | Cyber Security Specialist, Project Manager | |  | - Defect Tracking | Cyber Security Specialist, Project Manager | |  | - Test Summary Report | Cyber Security Specialist, Project Manager | |
| **Test Case** |
| | **Test ID:** | TC-0001 | | --- | --- |  |  |  | | --- | --- | | **Node List:** | Windows AD 2022 server VM on Azure cloud, pfSense VM |  |  |  | | --- | --- | | **Test Description:** | Perform a simple DDoS attack to assess the effectiveness of pfSense in mitigating such attacks. |  |  |  | | --- | --- | | **Test Phase:** | Baseline - DDoS Attack Testing |  |  |  | | --- | --- | | **Test Suite:** | | | The Baseline - DDoS Attack Testing test suite focuses on validating the fundamental network security capabilities of pfSense in mitigating Distributed Denial of Service (DDoS) attacks. This suite is specifically designed to assess the effectiveness of pfSense in handling and mitigating such attacks.  Test cases within the Baseline - DDoS Attack Testing test suite may include:   1. **DDoS Attack Simulation**: Simulate a variety of DDoS attack scenarios, such as SYN flood, UDP flood, or ICMP flood, to evaluate pfSense's ability to detect and mitigate these attacks. 2. **Attack Traffic Analysis**: Monitor and analyze network traffic patterns during the DDoS attack to assess how pfSense handles the incoming malicious traffic and distinguishes it from legitimate traffic. 3. **Traffic Throttling and Blocking**: Evaluate the effectiveness of pfSense's traffic throttling and blocking mechanisms in mitigating the impact of the DDoS attack on the network infrastructure and services. 4. **Performance Monitoring**: Measure the system's performance metrics, such as throughput, latency, and resource utilization, during the DDoS attack to ensure that pfSense maintains acceptable performance levels. 5. **Security Event Logging:** Verify that pfSense accurately logs DDoS attack events, providing useful information for forensic analysis and identifying potential vulnerabilities or patterns.   The Baseline - DDoS Attack Testing test suite is specifically focused on evaluating the baseline behavior of pfSense when subjected to DDoS attacks. It aims to determine how well pfSense can detect, mitigate, and handle these attacks to establish a reference point for subsequent performance improvements or optimization strategies. | | | **Test Setup:** | | | The test setup involves a virtual environment hosted on Azure, comprising a Windows AD 2022 server VM and a pfSense VM. The pfSense VM acts as a virtual switch between the internet and the Windows AD server, providing network security and firewall functionality.  **Hardware:**  **Virtual Machines:**  Windows AD 2022 server VM: Running on Azure cloud infrastructure.  pfSense VM: Running on Azure cloud infrastructure.  **Logical Configurations:**  **Windows AD 2022 server VM:**  Configure Windows AD with an active directory domain environment.  Set up necessary network settings, including IP addresses, subnet masks, and gateway configurations.  Configure appropriate security settings, such as firewall rules and access controls.  **pfSense VM:**  Deploy pfSense as a virtual machine on Azure.  Configure network interfaces on pfSense, ensuring proper connectivity between the internet and the Windows AD server.  Set up pfSense firewall rules to allow necessary traffic and provide network security.  **Test Tools:**  **DDoS Testing Tool:** A specialized tool capable of generating simulated DDoS attacks. Examples include hping, LOIC (Low Orbit Ion Cannon), or custom scripts that can generate high-volume traffic.In this case, we will be using nmap to flood the target, in hope of returning a response that prevents this  **Applications/Services:**  **Hyper-V Manager:** Utilized to manage the virtual machine environment, including the creation and management of VMs.  **Azure Cloud Infrastructure:** Provides the underlying platform for hosting the virtual machines and networking infrastructure.  **Diagram**:    The above diagram illustrates the test setup, showcasing the logical connectivity between the internet, the pfSense VM, and the Windows AD 2022 server VM. The pfSense VM acts as a virtual switch between the internet and the Windows AD server, providing network security and firewall functionality.  Before executing the test, we’ll ensure that the virtual machines are properly provisioned and configured, the necessary network connectivity is established, and the required logical configurations and security settings are in place. This test setup provides the foundation for conducting the desired tests related to network security and DDoS attack mitigation. | | | **Test Steps:** | | | Ensure that the test environment is properly set up with the Windows AD 2022 server VM and pfSense VM.  Install and configure nmap on a separate machine outside the test environment. This machine will be used to simulate the DDoS attack.  Identify the target IP address of the Windows AD 2022 server VM within the test environment.  Execute the following nmap command to simulate a DDoS attack:  nmap -Pn -p 80 --max-parallelism 100 --min-parallelism 10 --max-rate 1000 --send-eth -S 192.168.0.103 -f -g 53 --data-length 100 <target IP>  **-Pn**: Treat the target host as online, skipping host discovery.  **-p 80**: Specifies the port to target (e.g., port 80 for HTTP).  **--max-parallelism 100**: Set the maximum number of parallel probes to send.  **--min-parallelism 10**: Set the minimum number of parallel probes to send.  **--max-rate 1000**: Limit the sending rate of packets to 1000 per second.  **--send-eth**: Use raw Ethernet socket for sending packets.  **-S 192.168.0.103** : Specifies the source IP address to use for the attack packets, in this case a Kali Linux machine.  **-f** : Fragment the packets to evade detection.  **-g 53**: Set the source port to 53 (DNS) to bypass some firewall rules.  **--data-length 100**: Set the payload length of the attack packets to 100 bytes.  **192.168.1.100**: The target IP address of the Windows AD 2022 server VM.  Monitor the network traffic and behavior of pfSense and the Windows AD server during the simulated DDoS attack.  Observe how pfSense handles the attack by examining its logs, traffic patterns, and any detected anomalies or blocked packets.  Assess the impact on the Windows AD server, such as any disruptions in services or degraded performance.  Document the observed results, including any deviations from the expected behavior.  Repeat the test with different parameters or attack scenarios to evaluate pfSense's effectiveness in mitigating DDoS attacks.  Once the test is completed, analyze the test data, including performance metrics, logs, and any identified issues or vulnerabilities. | | | **Expected Results:** | | | **pfSense should detect the DDoS attack**: The logs and monitoring systems of pfSense should indicate the detection of the DDoS attack. This can be observed through increased traffic, abnormal patterns, or identified anomalies.  **pfSense should mitigate the attack**: pfSense should respond to the DDoS attack by implementing appropriate measures to mitigate its impact. This may include dropping or blocking malicious packets, rate limiting traffic, or activating specific firewall rules.  **Network performance remains stable:** Despite the DDoS attack, the network performance should remain stable and unaffected to a significant extent. There may be a slight degradation due to increased traffic, but it should not lead to complete network unavailability or severe performance degradation.  **Windows AD server continues functioning**: The Windows AD 2022 server should continue to function normally during the DDoS attack. There should be minimal impact on the services provided by the server, such as authentication, authorization, or resource access.  **Attack packets are identified and blocked**: pfSense should successfully identify the attack packets and take appropriate actions to block or drop them. This can be observed through the logs or monitoring systems, which should indicate the blocked packets or the corresponding actions taken by pfSense.  **No service disruptions on the Windows AD server**: The DDoS attack should not cause any significant service disruptions on the Windows AD server. Services provided by the server, such as user authentication, directory services, or DNS resolution, should remain operational without major interruptions.  **The network returns to normal after the attack:** Once the DDoS attack subsides or mitigation measures take effect, the network should return to its normal state with traffic patterns and performance returning to baseline levels. | | | **Observed Results:** | | | Based on the provided firewall log entry in pfSense, the observed result is as follows:  **Observed Result:**  The log entry indicates that pfSense blocked a network traffic flow originating from the WAN (Wide Area Network) interface towards the private network with the IP address range of 192.168/16 (192.168.0.0 to 192.168.255.255). The specific traffic flow was identified as a UDP (User Datagram Protocol) communication.  **Detailed Explanation:**  **Log Timestamp:** "Jun 27 00:04:33"  Indicates the date and time when the event occurred. In this case, the event occurred on June 27th at 00:04:33.  **Interface**: "WAN"  Specifies the network interface through which the traffic was received. In this case, the traffic was coming from the WAN interface, which is the external-facing interface connected to the internet.  **Block Rule:** **"Block private networks from WAN block 192.168/16 (12004)"**  Indicates the specific firewall rule that caused the blocking action. In this case, it is a rule configured in pfSense to block traffic from private networks (in this case, the 192.168/16 network range) when it arrives from the WAN interface.  **Source IP and Port**: "192.168.0.100:5353"  Specifies the IP address and port number from which the traffic originated. In this case, the source IP address is 192.168.0.100, and the source port is 5353.  **Destination IP and Port**: "224.0.0.251:5353"  Indicates the IP address and port number of the destination for the blocked traffic. In this case, the destination IP address is 224.0.0.251, which is a multicast address commonly used for mDNS (Multicast DNS) services, and the destination port is 5353, which is the standard port for mDNS.  **Protocol: "UDP"**  Specifies the transport protocol used by the traffic flow. In this case, it is UDP, which is a connectionless protocol often used for quick and lightweight data transfers.  **Summary:**  The observed result indicates that pfSense detected and blocked network traffic from the WAN interface to the private network range 192.168/16. Specifically, the log entry shows the blocking of UDP traffic originating from the IP address 192.168.0.100 on port 5353, targeting the multicast address 224.0.0.251 on the same port. This action is in line with the configured firewall rule in pfSense, which aims to prevent private network traffic from reaching the WAN interface. | | | **Pass/Fail:** | Based on the provided information, we can assess the test result as follows:    **Pass/Fail**: **Pass**  Based on the observed result and the nature of the firewall log entry, it indicates that pfSense successfully blocked the DDoS network traffic from the WAN interface to the private network range of 192.168/16. This aligns with the expected behavior and the configured firewall rule in pfSense.  Since the observed result matches the expected behavior, we can consider the test result as **Pass**. | |