**EQUIPMENT TEST PLAN**

**Sophos Firewall - Linux 2 Web Server**

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

|  |
| --- |
| **Overall project scope and objectives** |
| The objective of the AWS CyberShift Initiative project is to enhance the security of OzCazual's cloud infrastructure and facilitate a seamless migration from their current local server to Amazon AWS.  The key objectives are as follows:   * Mitigate the challenges arising from a sudden 200% surge in online sales and staff. * Establish a scalable infrastructure capable of accommodating future business requirements. * Safeguard the confidentiality, integrity, and availability of systems and customer data. |
| **Test objectives and success criteria** |
| **Test Objectives:**   1. Verify the successful deployment of Sophos XG as a cloud-based virtual machine, ensuring compatibility and seamless integration with the selected cloud platform (e.g., AWS, Azure, Google Cloud). 2. Evaluate the effectiveness of Sophos XG in securing network traffic, encompassing firewall rule configuration, NAT setup, VPN connectivity, and traffic monitoring capabilities. 3. Assess the scalability of Sophos XG in the cloud environment, taking into account factors such as increased network traffic, user count, and resource utilization. 4. Test the failover and high availability capabilities of Sophos XG in the cloud, ensuring uninterrupted network security and availability during failure or maintenance events. 5. Validate the interoperability of Sophos XG with other cloud-based services like load balancers, DNS services, or cloud storage, ensuring seamless integration and functionality. 6. Evaluate the logging and reporting capabilities of Sophos XG, verifying accurate log generation and availability of relevant information for monitoring, troubleshooting, and compliance purposes. 7. Test the resilience of Sophos XG against common network attacks, including Denial of Service (DoS) attacks, port scans, and intrusion attempts, to confirm its effectiveness in threat detection and mitigation. 8. Assess the ease of management and configuration of Sophos XG in the cloud environment, including features such as remote access, web-based administration, and automation capabilities.   **Test Network :**   1. Ensure the successful deployment of Sophos XG as a cloud-based virtual machine, without encountering any compatibility issues or setup errors. 2. Verify the functionality of essential Sophos XG features, including firewall rules, NAT configuration, VPN connectivity, and traffic monitoring, in conjunction with the Linux Web Server. 3. Assess the performance of Sophos XG in terms of throughput, latency, and resource utilization, ensuring it meets the requirements of the intended network environment. 4. Establish effective network security with Sophos XG, blocking unauthorized access attempts and filtering network traffic according to defined rules and policies. 5. Evaluate the scalability of Sophos XG in the cloud environment, ensuring it can handle increased network traffic, additional users, and resource demands while maintaining performance and stability. 6. Seamlessly integrate Sophos XG with other cloud-based services such as load balancers, DNS services, or cloud storage, ensuring compatibility and uninterrupted functionality. 7. Validate the failover and high availability capabilities of Sophos XG, guaranteeing uninterrupted network security and availability during failure or maintenance scenarios. 8. Ensure accurate logging and reporting of network activities by Sophos XG, providing valuable information for monitoring, troubleshooting, and compliance purposes. 9. Verify the effectiveness of Sophos XG in detecting and mitigating common network attacks, ensuring the network remains protected and secure. 10. Enable user-friendly management and configuration of Sophos XG in the cloud environment, leveraging features such as remote access, web-based administration, and automation capabilities to 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 Sophos XG 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 Linux Web Server Server as the test environment. * **Sufficient compute resources:** Ensure that the virtual machine has adequate CPU, memory, and storage resources to run Sophos XG and accommodate the expected network traffic. * **Software: Sophos XG:** Install and configure Sophos XG as a virtual machine on the Azure virtual machine. * **Linux Web Server:** Set up and configure Linux Web Server on the virtual machine to test the integration with Sophos XG. * **Hyper-V Manager:** Utilize Hyper-V Manager to manage the virtual machine and virtual network settings. * **Testing Tools:** * **Network traffic generator:** To simulate different network traffic scenarios and assess the performance of Sophos XG. * **Network monitoring and analysis tool:** To capture and analyze network traffic passing through Sophos XG for security and performance evaluation. * **Vulnerability scanner:** To test the effectiveness of Sophos XG in detecting and mitigating common network vulnerabilities. * **Load testing tool:** To evaluate the scalability and performance of Sophos XG under high network traffic conditions. * **Logging and reporting tools:** To capture and analyze logs generated by Sophos XG 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. | |
| **Test schedule** |
| The testing schedule outlines the roadmap for evaluating Sophos XG, a network security solution, in a cloud-based virtual machine environment with Linux UBuntu Web Server. It defines key milestones, dates, and resource allocations for each phase of the testing process. The main purpose of the test schedule is to provide a structured approach for planning, executing, and reporting the test activities. It ensures that the necessary resources, including personnel and hardware, are appropriately allocated throughout the testing process. The schedule helps manage timelines, dependencies, and milestones, promoting efficient coordination and communication among team members involved in the testing effort.  Following the test schedule allows the team to methodically progress through different phases, including test planning, environment setup, test execution, and reporting. This approach ensures comprehensive evaluation of essential aspects such as performance, security, scalability, and interoperability, with proper documentation. The test schedule maintains visibility into the testing progress and facilitates timely reporting of results, enabling informed decision-making and ensuring the reliability and effectiveness of Sophos XG 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 Linux Web Server | System Administrator | |  | - Deploy Sophos XG 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:** | LS-001 |
| **Node List:** | Linux Ubuntu Server 23.04 on Azure cloud, Sophos XG VM |
| **Test Description:** | Perform a simple DDoS attack to assess the effectiveness of Sophos XG 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 Sophos XG in mitigating Distributed Denial of Service (DDoS) attacks. This suite is specifically designed to assess the effectiveness of Sophos XG 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 Sopho'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 Sophos XG handles the incoming malicious traffic and distinguishes it from legitimate traffic. 3. **Traffic Throttling and Blocking**: Evaluate the effectiveness of Sopho'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 Sophos XG maintains acceptable performance levels. 5. **Security Event Logging:** Verify that Sophos XG 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 Sophos XG when subjected to DDoS attacks. It aims to determine how well Sophos can detect, mitigate, and handle these attacks in order 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 Linux server VM and a Sophos XG. The Sophos XG VM acts as a virtual switch between the internet and the Linux Server, providing network security and firewall functionality.  **Hardware:**  **Virtual Machines:**  Linux Web Server: Running on Azure cloud infrastructure.  Sophos XG: Running on Azure cloud infrastructure.  **Logical Configurations:**  **Linux Web Server:**  Set up necessary network settings, including IP addresses, subnet masks, and gateway configurations.  Configure appropriate security settings, such as firewall rules and access controls.  **Sophos XG:**  Deploy Sophos XG as a virtual machine on Azure.  Configure network interfaces on Sophos XG, ensuring proper connectivity between the internet and the Linux Web server.  Set up Sophos XG 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**:  **Data passes through Sophos**  The above diagram illustrates the test setup, showcasing the logical connectivity between the internet, the Sophos VM, and the Linux Web server VM. The Sophos VM acts as a virtual switch between the internet and the Linux Web 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:** | |
| 1. Ensure that the test environment is properly set up with the Linux Web server VM and Sophos VM. 2. Install and configure nmap on a separate machine outside the test environment. This machine will be used to simulate the DDoS attack. 3. Identify the target IP address of the Linux server VM within the test environment. 4. 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 192.168.56.200 -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 192.168.56.200** : 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.  **192.168.56.201**: The target IP address of the Linux Web server VM.   1. Monitor the network traffic and behavior of Sophos XG and Linux Web server during the simulated DDoS attack 2. Observe how Sophos XG handles the attack by examining its logs, traffic patterns, and any detected anomalies or blocked packets. 3. Assess the impact on theLinux Web server, such as any disruptions in services or degraded performance. 4. Document the observed results, including any deviations from the expected behavior. 5. Repeat the test with different parameters or attack scenarios to evaluate Sophos XG's effectiveness in mitigating DDoS attacks. 6. Once the test is completed, analyze the test data, including performance metrics, logs, and any identified issues or vulnerabilities. | |
| **Expected Results:** | |
| **Sophos XG should detect the DDoS attack**: The logs and monitoring systems of Sophos XG should indicate the detection of the DDoS attack. This can be observed through increased traffic, abnormal patterns, or identified anomalies.  **Sophos XG should mitigate the attack**: Sophos XG 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.  **Linux Web Server server continues functioning**: The Linux Web Server 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**: Sophos XG 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 Sophos XG.  **No service disruptions on the Linux Web Server server**: The DDoS attack should not cause any significant service disruptions on the Linux Web Server 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 firewall log entry in Sophos XG, the observed result is as follows:  **Observed Result:**  The log entry indicates that Sophos XG 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:** "July 09"  Indicates the date and time when the event occurred. In this case, the event occurred on July 9th at 00:14:25.  **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 Sophos XG 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:**  Based on the observed outcome, it is evident that Sophos XG successfully identified and obstructed network traffic from the WAN interface towards the private network with the range 192.168/16. The log entry specifies that UDP traffic originating from the IP address 192.168.0.100 on port 5353 was blocked. The target of this blocked traffic was the multicast address 224.0.0.251, using the same port. This action aligns with the firewall rule configured in Sophos XG, which intends to restrict any private network traffic from accessing the WAN interface. | |
| **Pass/Fail:** | Based on the provided information, we can assess the test result as follows:  **Pass/Fail**: **Pass**  Upon reviewing the outcome and analyzing the firewall log entry, it is evident that Sophos XG effectively thwarted the DDoS network traffic originating from the WAN interface and targeting the private network range of 192.168/16. This outcome aligns seamlessly with the anticipated behavior and the firewall rule that was set up in Sophos XG.  Considering that the observed result corresponds precisely to the expected behavior, we can confidently conclude that the test result is a success. |