To enable the default Security Profile Group for Brute force attack mitigation on vm-series

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Created By** | **Reviewer** |
| V1 | 5-NOV-2024 | Aishwarya Joshi | Akshay Mishra, Aashish Kumar |

*Document Version History*

|  |  |
| --- | --- |
| **Change Request** | |
| **Change Reference No.** | CHN-170 |
| **Subject** | To enable the default Security Profile Group for Brute force attack mitigation on vm-series |
| **Description** | A Brute force attack was observed and detected on the production environment on 13/09/2024 and 21/10/2024. This Brute force attack was detected on the CN-series firewalls. |
| **Reason for Change** | By selecting the security profile group as “VM-Security-Profiles-Group” for both security rules “Allow VPN traffic On-prem to AWS “and “Allow VPN traffic AWS to On-prem", Brute force attack will be detected and alerted on the VM-series firewalls. |
| **Impact** | Need to monitor traffic and threat logs and verify the security profile group applied on the “Allow VPN traffic On-prem to AWS “and “Allow VPN traffic AWS to On-prem". |
| **Components changed during CR** | Palo Alto Panorama Security Policies |
| **AWS/OEM Reference** | Palo Alto support team |
| **Business/Service Impact** | The absence of brute force detection and alerting measures on the VM-series firewalls exposes the production environment to increased security risks, as unauthorized access attempts may go undetected. This vulnerability could lead to potential data breaches, unauthorized access, and compromised system integrity, impacting the organization’s security posture and potentially leading to regulatory non-compliance. Implementing comprehensive brute force detection across both CN-series and VM-series firewalls is essential to ensure consistent security controls, reduce risk exposure, and safeguard sensitive data and operations. |
| **Rollout Plan** | This attached rollout plan includes the steps required for applying the changes in the security rules. |
| **Backout Plan** | If we still find any issue with the modifications on the security pre rules, we will simply revert changes by selecting the security profile group as “none” for both security rules “Allow VPN traffic On-prem to AWS “and “Allow VPN traffic AWS to On-prem". Followed by commit and Push changes to the devices, that will revert the changes and stabilize the system in the previous state. |
| **Pre-prod Test Result** | NA |
| **Any Downtime** | The changes applied to the security rules may alert brute force attacks for connections sending more than 100 requests per min. |
| **Resource carrying out change ( From both Ops and Hyper-care Team )** | Aashish kumar |
| **Schedule** |  |
| **Initiator** | Security team |
| **Approval from Accenture Lead/Manager** | Mihir, Aashish kumar |
| **Reviewer from IOCL** |  |
| **Approval from IOCL** |  |

Why we require this change

A brute force attack was observed and detected in the production environment on 13/09/2024 and 21/10/2024, specifically on the CN-series firewalls. Currently, the VM-series security rules lack a security profile group for detecting and alerting brute force attacks. Consequently, these attacks were only identified and alerted on the CN-series firewalls. Similar measures should be implemented on the VM-series firewalls to ensure comprehensive detection and alert for brute force attacks across all firewall series.

Implementation Plan

Log into Panorama Dashboard:

Step 1: Switch to SharedServices Account

<https://d-9f6701bb71.awsapps.com/start/#/>

A white rectangular object with a black border

Description automatically generated

Step 2: Navigate to EC2 Instances in Mumbai region

Windows Bastion Server: i-0a1cc3283ed210633 (INMUABSWP002)

A screenshot of a computer

Description automatically generated

Step 3: Connect to EC2 instance via RDP client. Use the key pair for authentication.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

Step 4: Once logged in to the Bastion server, use below link for Panorama Account : [https://iras-panorama.iocliras.in](https://iras-panorama.iocliras.in/)

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Apply Security Profile Group for Security rules

Step 1: Review the Security Policy Group, navigate to Objects Tab, Under Security Profile Groups, switch Device group to “AWS-VM-Series-FW” and review the “VM-Security-Profiles-Group" group.  A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Step 2: Navigate to Policies Tab, switch Device group to “AWS-VM-Series-FW”.  Under Security pre rules, make following changes in the rules “Allow VPN traffic On-prem to AWS “and “Allow VPN traffic AWS to On-prem".

A screenshot of a computer

Description automatically generated

Step 3: Select the rule, navigate to Action tab. Under Profile settings, select “Group” for Profile Type and “VM-Security-Profiles-Group" for Group Profile.  Once the group is selected click “Ok”.

A screenshot of a computer

Description automatically generated

Step 4: To commit and push changes to devices, navigate to Commit. To preview the changes, click on “Commit to Panorama”, add description comment and head to commit. Once commit is successful, Push the changes using “Push to devices”.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated