SSH (Secure Shell) is a cryptographic protocol used to securely access devices and manage systems over networks, protecting communications from interception and unauthorized access. In this network topology, SSH enables remote administration of infrastructure components, with the AAA VM, Debian VMs, and MikroTik router all participating—either as SSH servers, clients, or jump hosts, depending on their roles. The NAC router acts as a secure jump host for internal access, enhancing security for sensitive environments.

SSH Security Policy Overview

SSH security policy in this deployment emphasizes minimizing attack surface, enforcing strong authentication, and restricting access based on need. Public key authentication is mandatory for all users and devices, with password authentication disabled across the environment. The principle of least privilege is applied to all SSH access: only authorized users can connect, root logins are prohibited, and network device settings prevent SSH forwarding and tunneling unless explicitly required.

Security Measures for SSH Servers (Debian VMs, AAA VM, Backup Server)

- SSH servers require public key authentication; password logins are disabled to prevent brute-force and credential attacks.
- Root login is strictly prohibited, further reducing the risk of privilege escalation; administrative actions must use sudo from permitted user accounts.
- Only designated users are allowed access using “AllowUsers” and strict user management, and unnecessary accounts are regularly reviewed and removed.
- Strong encryption and key exchange algorithms are provisioned (e.g., `ssh-ed25519`, `curve25519-sha256`, `chacha20-poly1305`, `aes256-gcm`), mitigating cryptographic vulnerabilities.
- SSH servers only listen on required network interfaces, reducing exposure to external threats and mitigating the risk posed by accidental configuration.
- SSH session timeouts are enforced (`ClientAliveInterval`, `ClientAliveCountMax`) to automatically disconnect inactive sessions, reducing risk from unattended connections.
- SSHD configuration validation is performed before service reloads to prevent misconfigurations that could lock out administrators.
- SSH logs are maintained at “VERBOSE” level for audit trails and incident response.

Security Measures for SSH Keys and Workstations

- SSH keys are generated using strong, modern algorithms, and stored securely on workstations with restricted permissions for authorized personnel only.
- Key rotation and revocation policies are implemented: compromised keys are removed immediately from servers' authorized_keys lists.
- Keys used for jump hosts and server administration are distinct, reducing the impact should any key pair become compromised.
- Only public keys required for access are deployed to servers; unnecessary keys are periodically audited and removed.

Security Measures for NAC Router (Jump Host)

- The MikroTik NAC router is configured as a secure jump host, requiring key-based authentication for both direct router access and for jumping to internal servers.
- RouterOS disables legacy algorithms and enforces strong cryptography (`ip ssh set strong-crypto=yes`).
- Password-based authentication is deactivated once key-based logins are confirmed functional, reducing susceptibility to password theft and brute-force attacks.
- Private keys must be in PEM format for compatibility and are securely imported for authorized router operations only.
- Router configuration is periodically reviewed and validated against security best practices.

Operational and Monitoring Practices

- SSH server and client configurations are audited regularly to ensure compliance and detect unauthorized changes.
- Logs are monitored for anomalous events, including multiple failed logins, unexpected connections, or key-related errors.
- SSH software and dependent libraries receive regular updates to patch vulnerabilities and maintain a strong security posture.
- Access to SSH jump hosts and sensitive servers is strictly regulated and reviewed as part of onboarding, offboarding, and incident response.

This policy ensures that only authorized personnel access network devices and servers, with robust cryptographic protection and minimal exposure to external attacks.