NIC VPN Policy

Purpose

The purpose of this policy is to provide guidelines for connecting internal servers hosted in NIC to minimize potential exposure of unauthorized users. This policy defines the Remote Access policy to access Servers hosted in NICNET from Internet over IPSec or SSL.

1.0 Scope

This policy applies to all authorized VPN users intending to access servers or applications hosted in NIC managed data center for remote administration and applications access.

2.0 Policy

Introduction

A **virtual private network** (VPN) has being traditionally used to connect remote users and branch offices to the corporate office over Internet as an alternative to expensive WAN connections to access sensitive data. VPN creates a virtual "tunnel" connecting two endpoints by encrypting end to end communication and protecting the data from unauthorized access or interception. Telecommuters and mobile users, who require seamless access to corporate network for regular work, can use IPSec VPN or Client based SSL VPN from any Internet Service Provider and access internal applications, do remote administration, monitoring and management of resources which are otherwise not accessible from Internet. Apart from these Clientless SSL VPN can provide secure access to sensitive applications as email, intranet Web application from Internet.

3.0 Responsibility

The user, site/server/ network administrator and NIC coordinator shall follow the policy.

3.1. VPN connection is provided to user online registration available in link http://vpn.nic.in Dully filled form has to be verified by HOD / reporting officer of concern ministry / department and forwarded through NIC Coordinator to VPN services division.

3.2. VPN connection is provided to authorize users from Ministries/Departments/Statutory Bodies/ Autonomous bodies of both Central and State /UT Governments. VPN connection is also provided to users from Departments as Banks/ PSUs who have hosted their servers in NIC / NICSI data centers as paid service. Access charges will be as per decided by competent authority.

3.3. VPN connection is provided for accessing the servers hosted in NIC managed data center for remote administration services and applications access. Administrative access means SSH, Telnet, FTP, RDP, Database or any other service which can be used change the system which can affect the service.

3.4. The Verification of the users shall be done by the authorized representative from the concerned department.

3.5. The concept of trust chain is the central theme. Trust chain consists of the user (applying for VPN), her/his Head of Department (HOD) / Reporting Officer (RO), NIC Coordinator for the respective department and the VPN team. The trust/responsibility of actions flows in this chain. It means that the VPN team trusts the NIC Coordinator only and is not concerned about the user or her/his HOD/RO. Conversely, the NIC Coordinator trusts the HOD/RO of the respective department and is not concerned about the user. The actions of the user is the responsibility of her/his HOD/RO

3.6. Server access requirement for user shall be checked by HOD / reporting officer as well as NIC VPN Coordinator before forwarding it to VPN services division.

3.7. There is two factor authentication of VPN user primarily as DSC issued by VPNCA or LDAP / OTP or biometric as per project requirement. Authentication can also be done using Digital Certificate issued by IDRBT, (n)Code.

3.8. VPN Log request as per NIC log policy. Sharing of log request will be from controlling officer / NIC coordinator with proper request and justification.

3.9. VPN account issued for one year if VPN needed for less than one year then user should clearly write the date till its needed and renewal of existing VPN can be done as per process of VPN renewal.

3.10. Revocation of VPN account and Digital certificate : The NIC coordinator has to inform VPN services division to disable/ suspend the vpn account and revoke the DC when the users leaves the organization before the term .

3.11. Once VPN connected, all traffic between the user's PC and VPN server will be through VPN tunnel and user will have access to the servers listed in the application form.

3.12. In case of specific requirements, simultaneous access to other NICNET sites can be provide on approval from competent authority. No internet access will be allowed after connection of VPN.

3.13. Users has to make sure that the client system used for VPN connection is regularly scanned and updated with latest IOS patches and anti-virus software.

3.14. Any change in the Web applications/ server IPs which are to be accessed through VPN, has to be intimated to the VPN services division.

3.15. Any issue can be reported through NIC Service Desk only. There are no dial-in numbers for VPN support. The users need to create a ticket at NIC Service Desk and the VPN support will call the users on the contact number provided in the ticket. All software, procedures and manuals are available at the website https://vpn.nic.in.

3.16. NIC will not be responsible of any activities done in the server / site even if the connection is established through remote VPN. The server administrator should take necessary precaution to secure their application/ server.

4.0 Enforcement

The policy has to be enforced by VPN administrators, site/server/ network administrator and NIC coordinators.