Name of the Document		*Remote Access VPN Policy*	
Classification	*Unclassified*	**Audience**	*NIC Users*
Version	*3.0*	**Data of last change**	*April 2015*
Status	*Draft*	**Document No.**	*NIC-INOC-POL-VPN-002*

Document Control

S. No.	Type of Information	Document Data
1.	Title	NIC VPN Policy
2.	Code	NIC-INOC-VPN-PO-1
3.	Date of Release	July-10
4.	Version No.	1
5.	Owner	Mr. R S Mani
6.	Author(s)	Mrs. Arpita Barman

Change History

Date	Version	Nature of Change	Author
1-Sept-2010	1.2	Insertion of point 3.1	Arpita Barman
1-Jan-2012	2	Major modification	Arpita Barman
1 – Arp-2015	3	Major modification	Arpita Barman

Control of Document

Referred Policies, Procedures & Forms		
Policies	**Procedures**	**Forms, Templates, Presentation**
NIC VPN Policy	Manual for configuring IPSec VPN client for Windows platform	Online VPN Registration form for new account, Renewal , change and Project
	Manual for configuring SSL VPN client	Authorization Form. Cloud Sign up form
		DCS-Request form

Name of the Document		*Remote Access VPN Policy*	
Classification	*Unclassified*	**Audience**	*NIC Users*
Version	*3.0*	**Data of last change**	*April 2015*
Status	*Draft*	**Document No.**	*NIC-INOC-POL-VPN-002*

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 authorized users of NIC intending to access internal servers or applications hosted in NIC for remote administration, Site and database updation or secure access to Intranet applications. This policy applies to VPN connections provided through centralized VPN servers.

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.

3.1. VPN connection is provided to user online registration available in link http://vpn.nic.in which has to be forwarded by HOD / Project Coordinator. VPN account is also provided for accessing cloud services on Signing up to http://clouds,gov.in.

3.2. VPN connection is provided to user for accessing the servers hosted in NICNET/ NKN for management, updation and monitoring. VPN connection is provided to access Intranet applications hosted in NIC IDCs.

3.3. VPN connection is provided to authorised users from Ministries/Departments/Statutory Bodies/ Autonomous bodies of both Central and State /UT Governments.

3.4. VPN connection is also provided to users from Departments as Banks/ PSUs who have hosted their servers in NIC / NICSI datacenters as paid service.

3.5. The Verification of the users shall be done by the authorised representative from the concerned department.

3.6. NIC coordinator is the authorised NIC employee to coordinate with concerned department/ sector/state/project.

3.7. VPN access will only be provided to servers hosted in NICNET/NKN and behind firewall.

3.8. Authentication of VPN user is primarily through Digital Certificate provided from NIC enterprise CA.

3.9. Authentication can also be done using Digital Certificate issued by CCA registered Sub CAs or NIC LDAP / OTP as per project requirement and the approval of competent authority.

3.10. All forms, procedures and documents related to VPN are available in http://vpn.nic.in.

3.11. 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.

3.5. The Digital certificate and VPN account issued for two years and renewal can be done as per the norms of NICA. The user has to inform NICCA administration if Digital certificate is compromised or corrupted to revoke the digital certificate.

3.6. Revocation of VPN account and Digital certificate : The project coordinator has to inform INOC and NICCA divisions to disable/ suspend the vpn account and revoke the DC when the users leaves the organization before the term .

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

3.8. In case of Project / specific requirements , simultaneous access to other sites if required can be provide on approval from competent authority .

3.9. 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 .

3.10. The VPN connection will be automatically disconnect after due to inactivity. The user has to login again.

3.12. The VPN client software will be provided by supplier of the VPN server and would be compatible for standard Operating systems. NIC would provide users with required manuals and procedures for standard deployments and off site support.

3.11. However the user can use their own VPN client software, but it should be compatible with NIC VPN servers. In case user uses proprietary VPN client software, configuration has to be done by them. The VPN client software or appliance used should comply with NIC VPN policy and compatible with NIC VPN Servers. Any customization required for the same shall be done by the user.

3.12 Any change in the Intranet Web Applications/ hostname which are to be accessed through SSL VPN, has to be intimated to the VPN administration.

3.0 Responsibility

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

4.0 Enforcement

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

Name of the Document		*Remote Access VPN Policy*	
Classification	*Unclassified*	**Audience**	*NIC Users*
Version	*3.0*	**Data of last change**	*April 2015*
Status	*Draft*	**Document No.**	*NIC-INOC-POL-VPN-002*

5.0 References

http://security.nic.in

http:// www.sans.org

http://clouds.gov.in