

GOVERNMENT OF INDIA
(Ministry of Home Affairs)
Communication & IT Directorate
CENTRAL RESERVE POLICE FORCE
EAST BLOCK-7, SEC-1, R.K. PURAM, NEW DELHI-110066
(Tele/Fax No-011-26107493, Email-Id: comncell@crpf.gov.in)

No. B.V-7-C/2024-25-C(NAC)


Dated, the 11/ Dec'2024

Subject:- REQUEST FOR COMMENTS OF STAKEHOLDERS /OEM/FIRMS ON Draft QRs & TDs of "Network Access Control".

1. The Draft QRs/TDs of "Network Access Control" is attached as **Appendix 'A'**. The OEMs/Vendors are requested to forward information of the product, which they can offer and also forward correct specifications of their system against each parameter. Only complied or not complied remarks will not be accepted. The firms are also requested to furnish the following details:-
 - Whether you are OEM/Vendor?
 - If vendor details of OEM.
 - Authorization certificate from OEM.
2. The required information/details may please be forwarded at the following addresses by **26 Dec'2024**.

Communication Directorate, CRPF
East Block-7, Sec-1, R.K. Puram, New Delhi-110066
Email: comncell@crpf.gov.in

3. An early response is requested.


{Ujjwal Kumar Singh, AC (QRs)}
For DIG (Equipment)
Communication & IT Branch
Directorate General, C R P F

Draft QRs/TDs of Network Access Control

SL No.	Specifications	Trial Directive
<p>The proposed solution shall meet the below specifications. Any hardware/software/licenses required to enable the functionality shall be provided from Day 1</p>		
A	Device Profiling and Visibility	
1	Automatic detection and categorization of endpoints for security and audit demands, regardless of device type.	Verification with OEM Tech brochure and Console Software
2	Stored profiling data should identify device profile changes and dynamically modify authorization privileges. <i>For example, if a printer appears as a Windows laptop, the system can automatically deny access.</i> should support Load balancing for profile scans and Scheduled Subnet scans	
3	Support passive device profiling methods such as DHCP, Span Ports, HTTP User-Agent, MAC OUI and TCP SYN-ACK handshakes	
4	Support active device profiling methods such as SNMP, Subnet Scan, SSH, Sflow, WMI and NMAP Scan	
5	Internal device fingerprint dictionaries that provide a way to automatically or manually update periodically. Capable to define custom fingerprints for wired and wireless devices	
6	Offer a comprehensive dashboard to see the total number of endpoints, and the number by category, family and device type.	
B	Authentication, Authorization and Accounting (AAA)	
1	Integrated scalable AAA services (authentication, authorization, and accounting) including access policy management with a complete understanding of context, such as user's role, device type, location, time of day etc.	Verification with OEM Tech brochure and Console Software
2	User and device authentication based on 802.1X, and Web Portal access methods across multi-vendor wired networks , wireless networks, and VPNs	

SL No.	Specifications	Trial Directive
3	Usage of multiple authentication protocols concurrently, such as PEAP, EAP-FAST, EAP-TLS, EAP-TTLS, and EAP-PEAP-Public.	Verification with OEM Tech brochure and Console Software
4	Must support RADSEC protocol to support RADIUS datagrams over TCP and TLS. Should be able to work on all major OEM network switches.	
5	Must be supplied with fine-grained control using attributes from multiple identity stores, such as Microsoft Active Directory, Kerberos, LDAP-compliant directory, Open Database Connectivity (ODBC)-compliant SQL database, token servers, and internal databases across domains within a single policy from day one	
6	Non-802.1X devices (such as printers, IP phones, IP cameras and IOT devices) can be identified as known, based on the presence of their MAC addresses in database, or unknown upon connecting to the network.	
7	Integrated TACACS+ server for secure authentication of device administrators, operators etc. with varied privilege levels. It should keep a track of the changes made by the logged-in user.	
8	Customizable Reporting with manual or scheduled reports in PDF/CSV formats, inventory dashboard showing details of learned devices, real-time monitoring of access requests and events, proactive alerts through Email	
9	HTTP/RESTful API's, syslog messaging and Extensions capability to exchange endpoint attributes with firewalls, SIEM, endpoint compliance suites and other solutions for enhanced policy management	
10	Mobile Device Management Integration to fetch information such as device manufacturer, model, OS Version, Jail-broken, presence of any black-listed application, MDM Agent installation status etc. and use this information in access policies	
11	API Integration with helpdesk software allowing dynamic creation of problem tickets of any network triggered policy breaches	
12	Inbuilt utilities for interactive policy simulation and monitor mode for assessing the policies before applying to the production network	

SL No.	Specifications	Trial Directive
13	Process inbound threat-related events (which are Syslog events received from any third-party vendor device, such as Firewall, SIEM) and perform enforcements and actions based on the defined enforcement policies and services.	Verification with OEM Tech brochure and Console Software
14	Must have Multi domain and multiple AD and user database support for user information	
15	All the user machines must be evaluated before allowed on the network and thus must only deploy with a secured IEEE 802.1X architecture	
C	Guest Access Management	
1	Easy-to-use guest management solution for visitors, contractors, partners, Auditors etc. on wireless and wired networks using any type of device.	Verification with OEM Tech brochure and Console Software
2	Guest access through captive portal with extensive branding and customization including company logos, visual imagery and optional advertisements with multimedia content to extend organization's messaging	
3	Captive portal (Responsive Design to support different screen size) should have mobile device awareness to automatically size for smart phones, tablets and laptops	
4	Guest self-registration through the web portal, delivering username and password directly to the visitor's Web browser, or sent via email or SMS.	
5	Sponsor-based approval workflow to enable an internal employee to approve guest account before guest is allowed to access the network	
6	Customize guest access privileges to enforce bandwidth limits, access to specific resources, length of connections and set automatic account expiry after a specified number of hours or days	
7	Guest portal shall have an option to accept Social logins using Facebook, Twitter, Slack and other social media credentials.	
8	Third-party integration providing customizable workflows using rest-based API's for delivering streamlined registration and payment system integration	

SL No.	Specifications	Trial Directive
D	Personal Device (BYOD) Management	
1	Automatically configure and provision mobile devices such as Windows, macOS, iOS, Android, Chromebook, and Ubuntu, enabling them to securely connect to enterprise network. Support for atleast(No of Users defined by User Department) users on day one. Each user can have upto two devices and support Sponsor approval required option for Onboarding.	Verification with OEM Tech brochure and Console Software
2	Offer built-in certificate authority (CA) to secure device onboarding without requiring the implementation of an external CA or make changes to an internal public key infrastructure (PKI). Incase for some reason any OEM unable to provide inbuilt CA then can provide it externally, however from day one . should work as a Root or Intermediate CA and support Self help portal for certificate management	
3	Support the distribution of in-built CA generated certificates to third-party applications using SCEP and EST (RFC 7030) protocols.	
4	Ensure rapid revocation and deletion of certificates for specific mobile devices if a user leaves the organization or the mobile device is lost or stolen.	
5	Support Online Certificate Status Protocol (OCSP)	
6	Capable to define the number of devices that can be on-boarded per user and validity of their certificates	
7	Automatic device certificate provisioning/installation with sponsor approval required option for onboarding	
8	Certificate Provisioning must work even after failover of its nodes	
9	Must support Oauth and SAML 2.0 Identity Provider, which allows seamless single sign-on (SSO) to the cloud or on premise applications.	

SL No.	Specifications	Trial Directive
10	Must support multiple multi-factor authenticators (MFA/2FA)	Verification with OEM Tech brochure and Console Software
	Should support Secure certificate based onboarding and Automatic device certificate provisioning / installation	
E	Endpoint Posture Checking	
1	Support Perform advanced endpoint posture assessments to ensure organization's compliance is met before devices connect	Verification with OEM Tech brochure and Console Software
2	Support the following operating systems and versions: Microsoft Windows 7 and above, Apple macOS 10.10 and above	
3	Support Users of unhealthy endpoints that do not meet compliance requirements, should receive a message about the endpoint status and instructions on how to achieve compliance	
4	Support Endpoint posture and health checks should include Installed Applications, Antivirus, Firewall, Network Connections, Processes, Patch Management, Peer to Peer applications, Virtual Machines, USB Devices etc.	
5	Support to persistent agent for operating system to provide nonstop monitoring of the end point with automatic remediation and control	
6	Support Offer web-based dissolvable agent for endpoint compliance check of personal and non IT-issued devices	
7	Must support detect multiple network interfaces and Control it	
8	Must support detect USB, disable it and remove it	
9	The solution must ensure standard based Zero Trust access network security framework with 24/7 network policy compliance checking and enforcement.	

SL No.	Specifications	Trial Directive
F	Management and Reporting	
1	Predefined templates for reporting must be available	Verification with OEM Tech brochure and management Software
2	Solution must have built-in monitoring, reporting, and troubleshooting console to assist helpdesk operators and administrators streamline operations.	
3	Solution must collect and keep forensic evidence on any unauthorized access activity within the network as follow: Event timestamp, network events in sequence, host info, IP address, MAC address, switch info, etc.	
4	Solution must support capability to generate report for hardware (Memory, RAM, HDD, Peripheral devices, etc.), All installed software with version, Open ports, Service Running, Process Running and application inventory across managed extended enterprise.	
5	Solution must be able to display information notifications in an interactive manner viz. bubble notification, email, etc.	
6	The NAC solution should be able to integrate with Nextgen SIEM and other SOC components.	
7	The proposed NAC solution should provide user-friendly policy management (policy search, policy updates, import/ export policies, etc.)	
8	A reporting option must be available to provide a method for delivering validated templates to unique requirements in a timely manner.	
9	Understanding trends, compliance and forensic analysis requires the ability to generate reports on data from selectable time frames in the past as well as on current data i.e. Specific date and time range	
10	In order to provide the information needed to make decisions and minimize data overload reporting systems must provide robust filtering options.	
11	Must have support for notifications via Email	
12	Web-based user interface that simplifies policy configuration, monitoring and troubleshooting	

SL No.	Specifications	Trial Directive
G	Capabilities with Existing Unmanaged Switches	
	The Proposed NAC solution should be able to detect the endpoint at the instant it connects to Customer network	Verification with OEM Tech brochure and management Software
	The Proposed NAC solution should be able to restrict communication to a non-compliant device which is connected to a hub/unmanaged switch, while another compliant device which should remain functional.	
H	Capability of building complete device inventory & context.	
1	Solution should maintain an up-to-date/centralized inventory of authorized devices connected to network and authorized devices enabling the network	Verification with OEM Tech brochure and management Software & reporting tool
2	Solution must provide true-up enterprise endpoint data with complete device inventory & context in automated manner.	
3	Solution must be able to provide compliance for Hardware properties on windows like Hardware Computer, Disks, Monitors, Motherboard, Network Adapter, Physical Device, Physical Memory, Plug and Play Device, Processor, etc.	
4	Solution must automate the inventorying of IP-connected assets across extended enterprise networks along with detailed information of hardware viz. Disks, Monitors, Motherboard, Network Adapter, Physical Device, Physical Memory, Plug and Play Device, Processor, etc. Pinpoint the real-time location of all IP-connected things, Continuously and accurately assess all IP-connected devices.	

SL No.	Specifications	Trial Directive
I	Requirement Summary	
1	The solution should be based Hardware appliance. The solution must support minimum 500 (Number defined by User Department) endpoint support from Day-1.	Verification with OEM Tech brochure and management Software
2	The solution shall support minimum 200 authentications per second for 802.1x/RADIUS/TACACS+/Guest and minimum 50 clients/second for endpoint posture checking	
3	Licenses supporting minimum 500 (Numbers decided by User department) concurrent sessions for AAA, Endpoint posture check, Guest access, (Numbers decided by User department) Endpoint Profiling and (Numbers decided by User department) BYOD devices from day-1. Solution Should scalable as per user department.	Verification with OEM Tech brochure and management Software
4	5-Year 24x7 Hardware and Software Warranty with perpetual / subscription licenses.	Verification with OEM Tech brochure and management Software
H	OEM and Product Eligibility/Compliance	
1	The solution shall be Common Criteria certified for network access control (NAC) solution, under both the Network Device collaborative Protection Profile (NDcPP) and the Extended Package for Authentication Servers modules. The certificate shall be attached as reference	firm will provide OEM Certificate.
2	OEM shall have R&D facility in India; if required site visit shall be arranged	
3	AAA shall be offered with minimum five years hardware warranty with 24X7 OEM direct support along with software updates/upgrades	
4	Optional : On Site OEM certified Engg. (Be decided by user department)	