EXPRESSION OF INTEREST FOR ADVANCE CYBER SECURITY SOLUTION FOR IMPLEMENTATION OF IT POLICY AND CYBER-SECURITY ON IT INFRASTRUCTURE OF CSIR-NEIST, JORHAT

CSIR-North East Institute of Science and Technology (NEIST) is a National Laboratory engaged in R&D under the aegis of Ministry of Science & Technology, Govt. of India. CSIR-NEIST is interested to have Advance Cyber Security Solution for Implementation of IT Policy and Cyber-Security on IT Infrastructure of CSIR-NEIST, Jorhat, Assam.

The required components having tentatively 500 end points for the above are given below:

1. **Next Generation Firewall in HA Mode.**
2. **End Point Management System**
3. **Centralised User Authentication for Wireless Network.**
4. **Centralised Network Access Control**
5. **Logging, Analysing and Reporting System**

(Note: 500 endpoints are tentative; hence the solution must have the scope for expansion to accommodate increased endpoints in the future.)

Terms & Conditions:

1. The interested bidders who want to participate in the EOI and who have some prior experience, are requested to submit their EOI through e-Tender or through mail (spo@neist.res.in) up to 11th January, 2021 with the following documents (scanned copy):
   (A) **Technical Offer with related details**
   (B) **Documents related with concerned technical literature/brochure**
   (C) **Documents of prior experience in the related field**
   (D) **Declaration on Land Border Sharing Countries with India in the given format (on letter head)**
   (E) **Self Certification for Make in India that at least 20% Indian Content is there in the offered system (on letter head) in the given format**

2. The offers will be evaluated first on the basis of the technical credential of the party, if required presentation will be taken from the parties.

3. On the basis of their presentation, technical submission and other aspects, it may be decided to ask the price quotation from the selected parties,

   Or

   This may be given for Open tender for other vendors' participation also as per decision of the competent authority. CSIR-NEIST, Jorhat authority reserves the right to take decision on the above.

भंडार एवं क्रय अधिकारी
Stores & Purchase Officer
For and On Behalf of the Council of Scientific & Industrial Research
Tel: 91 – 0376 – 2372710, E-mail: spo@neist.res.in

STATEMENT OF REQUIREMENTS FOR IMPLEMENTATION OF IT-POLICY AND CYBER SECURITY

The components required for the implementation of IT Policy and Cyber-Security on IT infrastructure of CSIR-NEIST having 500 endpoints* are given below: -

1. Next Generation Firewall in HA mode.
2. End Point Management System.
3. Centralised User Authentication for Wireless Network.
4. Centralised Network Access Control.
5. Logging, Analysing and Reporting System.

(*500 Endpoints are tentative, hence the solution must have the scope for expansion to accommodate increased endpoints in the future.)

1. Current Scenario and Problem Statement:

1.1 Present firewall is capable of handling current users load but unable to detect zero-day vulnerabilities, such as anomalies or malware, those are unknown and have not yet been discovered.

1.2 Due to performance issues, storage of network activity logs is not possible in existing firewall.

1.3 When it comes to web filtering and application filtering, the existing firewall does not contain enough signatures to determine all of the sites and applications that need to be blocked due to lack of advanced application layer security features.

1.4 Zero visibility and control on endpoints as no centralised solutions are in place.

1.5 Wi-Fi network are vulnerable due to uncontrolled sharing of pass key, as a result difficult to restrict unwanted network access.

1.6 Unable to pinpoint of any security breach in Network.

2. Objectives:

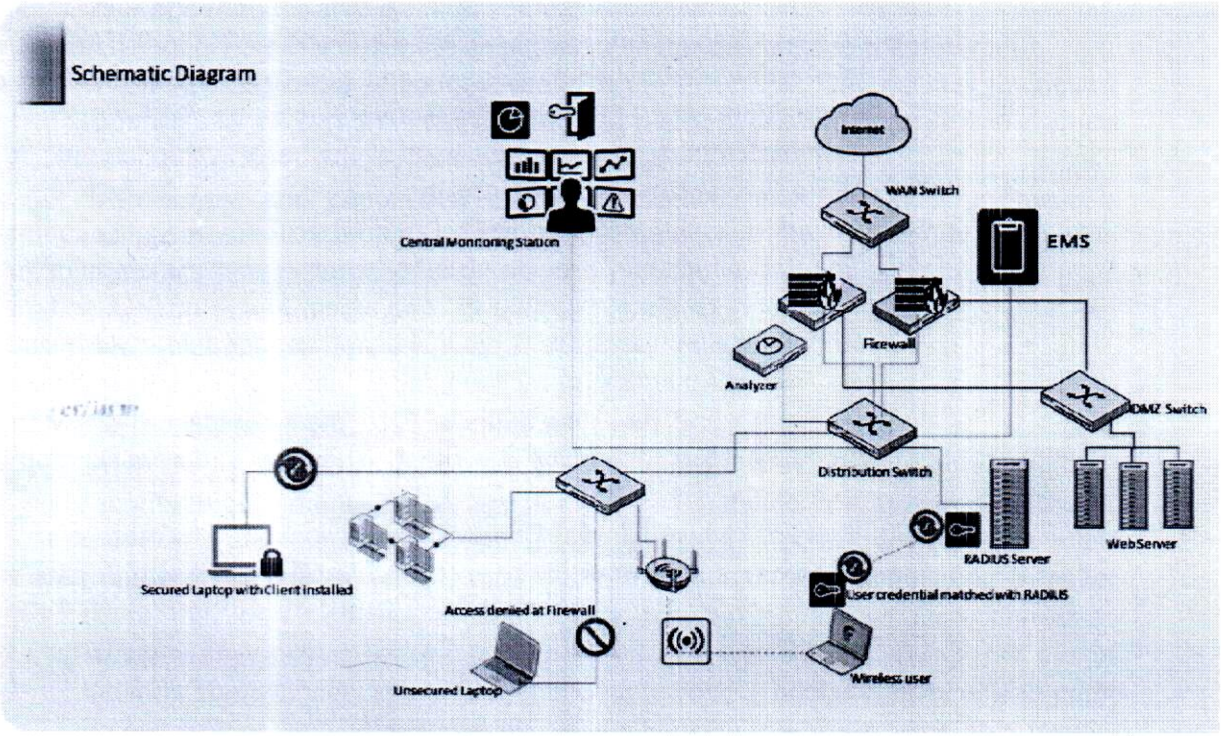
2.1 To implement a secured network in the institute, where there will be a complete visibility of entire network to ensure that, every endpoint in the network should be secured and compliant, any compromised host or non-compliant system should be blocked to gain network/internet access.

2.2 To change the current authentication method for Wi-Fi access, to have better control on users who are accessing wireless network.

2.3 To have centralised logging and reporting solution for entire network with greater visibility of the network and endpoint's health status which will help to isolate the root cause of the problem, if any and act promptly on that.

3. Proposed Requirements.

3.1



3.2 Brief description of the above diagram:

- 2(two) nos. Of Next-Gen Firewall will be placed at perimeter in HA mode where ISP/ISPs will be connected through a WAN switch for internet access.
- Other than LAN, a separate DMZ zone will be created to host WEB Servers. The servers will be connected to Firewall DMZ zone through DMZ Switch.
- Analyser is proposed for having a centralised Logging and Reporting Solution which will be connected to Core/Distribution switch.
- All the endpoints will be installed with Client/Endpoint protection. All endpoints will be managed by centrally EMS (Endpoint Management System), and the policy can be implanted to firewall so that non-compliant endpoint should not get access to the network/internet/DMZ zone. Only secured endpoints will be allowed.
- At present Web Servers are placed in the same LAN segment where all users are connected, which can be foresee as a security threat as any LAN user can have easy access to these Servers and as traffic are coming without any security scanning. Therefore, it is recommended to place the Web Servers under DMZ zone of firewall, so that every traffic originating from LAN to DMZ will be passing through firewall for security scanning and thus provide secured access to the servers.
- VLAN will be implemented to segregate the LAN for different users groups like guest, staff, administration and student. Implementation of VLANs will give

better control over the network in terms of security and congestion free network and, with different level of QOS (Quality of Service).

3.3 Endpoint Management System

- In any organisation, endpoints are always the most vulnerable target from the cyber security point of view, and due to non-availability of endpoint protection, the CSIR-NEIST's network are at high risk as System Administrator doesn't have visibility of the hosts in the network, so it is very difficult to ensure network security.
- To address this problem, it is required to implement Endpoint Security Solution which can provide visibility, control and proactive defences with the ability to discover, monitor, and assess endpoint risks and, can ensure endpoint compliance, mitigate risks, and reduce exposure including zero-day malware; botnet detections and vulnerability are reported in real-time. The deep and real time visibility into the network will allow the System Administrators to investigate and remotely quarantine compromised endpoints.
- Prevent known vulnerabilities from being exploited by attackers.
- Automated behaviour based protection against unknown threats.

3.4 Key Features required in Endpoint Management System

- Remote Client/Endpoint protection deployment.
- Automatic provisioning of new devices.
- Centralized client provisioning and monitoring.
- Dashboard providing endpoint alerts and summary.
- Vulnerability management.
- Software inventory management.
- Automatic Group Assignment.

3.5 Centralised User Authentication for Wireless Network:

- Implementation of RADIUS Server for centralised user authentication.
- Users have to provide unique credentials to access the wireless network
- The credentials provided by the user to access the wireless network are matched to the credentials stored in the directory which enforce to have unique and authenticated access to the wireless network.

3.6 Centralised Network Access Control:

- Implementation of Centralised Network Access Control to provide network visibility to see everything connected to the network, as well as the ability to control those devices and users, including dynamic automated responses.

3.7 Key Features required for Centralised NAC:

- **Visibility** - It should provide the deepest level of network endpoint visibility. It should profile every endpoint and infrastructure device on the network, and provides contextual awareness about the device, user, and applications. It also track and monitor all the activity on the network.

  Identifies IoT/headless devices each time a device connects to the network.

  When new device try to connect the Institute's network, NAC notifies the device sponsor/user to authorise the device onto the network and records every action (preserving user's privacy) taken by the device.

  With simple and centralised management, NAC ensure that if a device is compromised, it can be located promptly, even if the device is in remote location.
- **Control** – It should provide contextual awareness for scalable onboarding and dynamic network access control. Network access should be assigned using automated, predefined profiles – saving a significant amount of time when onboarding large numbers of students, guest, or staff to manage high volume of BYOD (Bring Your Own Device) devices, and help to set and enforce minimum security requirements for things like security patches and antivirus software. Using a pre-connect scan, NAC should grants access for devices that meet requirements and can automatically direct users to a self remediation page for those that don't qualify. It should also provide continuous post-connection scanning to look for devices and /or users that act suspiciously or fall out of network compliances. In addition, it should provide granular control of end-point access policies and permissions by role or by user to ensure users only receive the necessary amount of access and centrally managed end-to-end control of the entire fluid network, including satellite campus locations.
- **Intelligence** – Provide real-time automated threat responses that can be immediately quarantine any device that acts suspiciously.

3.8 Logging, Analysing and Reporting:

Log analysis and reporting is one of the major components of today's IT infrastructure. For the institute with large nos. Of users and endpoint accessing the Government internet and institutional intranet, it is difficult to look in to the entire network and to pinpoint of any incident which would adversely affect the security and reputation of the institute. Therefore, a centralised reporting solution is strongly recommended which can provide a robust reporting solution/platform which can collect logs from the firewall, Endpoint, Authenticator which will help to secure Institute's overall network by providing actionable views of log and threat data, using predefined and customised dashboards delivered through a single-pan-of-glass interface.

3.9 Required Key Features for logging, Analysing and Reporting Solution:

- Event correlation, threat detection and Indicator of compromise service to reduce time-to-detect and identify threats.
- Correlation with logs from Endpoint solution, Firewall and NAC for deeper visibility and critical network insights.

3.10 Next- Generation Firewall (NGFW):

NGFWs offer stateful inspection of traffic and a multifaceted range of security competencies plus features such as Intrusion Prevention Systems (IPS), web filtering, malware detection, URL filtering, encryption, and antivirus. These features are directly related to security and controlling what users and systems can do, along with preventing network attacks. It also allows businesses to prioritize what traffic is critical and what is not.

3.11 Required Key Features for NGFW:

- Protects against cyber threats with high-powered security processors for optimised network performance, security efficacy and deep visibility.
- Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement.
- Protect against malware, exploits and malicious websites in both encrypted and non-encrypted traffic.
- Proactively blocks unknown sophisticated attacks in real-time.
- Provide a management console that is effective and simple to use, which provides a comprehensive network of automation and visibility.
- Provide full visibility into users, devices, applications across the entire attack surface and consistent security policy enforcement irrespective of asset location.
- Protect against network exploitable vulnerabilities with industry-validated IPS that offers low latency and optimized network performance.
- Provide secure web access from both internal and external risks, even for encrypted traffic at high performance.
- Enhance user experience with dynamic web and video caching.
- Block and control web access based on user or user groups across URL's and domains.
- Prevent data loss and discover user activity to known and unknown applications.
- Block DNS request against malicious domains.
- Multi-layered advanced protection against zero-day malware threats delivered over the web.
