**1. How will you plan to scale your solution during the contract period as bandwidth and Internet usage requirements increase at the district level?**

    The NetSpective 12H model can handle up to 10 Gbps and will provide plenty of room for growth as your requirements increase.

**2. We see all types of devices being purchased and bought into school districts. How does your solution allow for traffic to be analyzed, filtered, prioritized, and reported on for various devices that may or may not currently be authenticating within the school district?**

    ​NetSpective monitors your network passively in what we refer to as Side Scan mode. NetSpective can see all network traffic, regardless of authentication or what port the traffic is going across. All unauthenticated devices can still be filtered under the Public Policy and have their web traffic restricted. If you wish for more granular filtering and reporting on these mobile devices, we can authenticate them in various ways, including the ability to present a captive portal for authentication to these devices.

**3. Our school districts have varying levels of technical expertise as it pertains to Internet filtering and management. What features does your solution contain that would assist customers of all skill levels as they attempt to manage their network environment as efficiently as possible?**

NetSpective offers a wide range of automation and ease of management features which make the system more approachable to customers of all skill levels. Abuse Detection can be set to automatically lock down users who attempt to surf objectionable traffic. Monitors and alerts can be set to send out automated emails when students try to search for objectionable search words.

Policy Templates were designed with simplicity in mind. Groups of users can be unified under one Policy Template. Any changes made to the template will affect all groups linked to the template, making changes to policy quick and easy. Templates can easily be duplicated and changed for school events and testing.

Management of the NetSpective can be delegated to individuals with less privileges, making the interface easier to navigate. Block Page Bypass managers can allow web pages through for students without the need to ever access the NetSpective Administration. Principals can utilize the Policy Manager role to change student policy and make website re-categorizations without seeing other menu options and settings that they do not need to manage. The Group Manager was designed with ISPs and Educational Service Centers in mind for delegating roles to downstream customers, while omitting features they shouldn’t have access to.

**4. How does your solution attach and retrieve information from Active Directory, meaning what TCP/UDP ports, protocols, etc?**

NetSpective can access the Active Directory tree structure with any user (not admin) credentials provided, across port 389. Port 389 is the standard port for LDAP (Lightweight Directory Access Protocol).

**5. What information in Active Directory does your solution utilize, and what does it do with that information?**

NetSpective is looking for organizational unit tree structure and uses that to populate NetSpective groups with DOMAIN/user names.

**6. Does your solution require any Active Directory schema changes?**

No, NetSpective will not require any AD schema changes.

**7. Describe any special network configurations and/or access permissions required beyond Active Directory Doman User?**

No special permissions or configurations are necessary beyond an AD domain user’s credentials.

**8. Several school districts have decided to filter internet traffic for district-owned devices when they leave the school campus; how does your solution handle filtering these devices, when they are no longer on the same campus/LAN.**

Our Remote Agents are designed for filtering and reporting on Windows and Mac OS X notebooks both on and off network. When installed on the user’s notebook, the remote agent will communicate back to the NetSpective appliance asking for a ‘Go’ or ‘No-Go’ on the user’s web traffic using a proprietary UDP packet. The appliance then checks against the user’s policy and sends that packet back to the remote agent to either allow the traffic or redirect to a block page. The user’s surfing history logs are sent back to the appliance periodically. Even if communication to the appliance is interrupted, the remote agent will hold log files until connection is restored. Our remote agents work intelligently alongside our logon agents and will deactivate themselves when the presence of the logon agent is detected so users on the LAN do not send logon information multiple times.

As a separate appliance that scales independently, the NetSpective Global Proxy is capable of filtering any device on or off the network. Devices such as iPads and Chromebooks that suspend applications or revert their image when restarted cannot be filtered with traditional agents. The Global Proxy can direct all traffic these devices generate back onto the network to ensure that school owned devices are filtered at home.

**9. Currently, schools have the option to enact different filtering rules on different schools (either through IP subnets or Active Directory group membership). How would your solution allow a district to have different filtering rules for different schools, while still maintaining an overall filtering policy (i.e. Global policy)?**

Filtering different schools through IP subnets or Active Directory will work the same as your functionality is today. NetSpective can support both authenticated filtering through Active Directory groups and organizational units, as well as specific policies for IP addresses or subnets. NetSpective also offers a Public Policy, which ensures any remaining unauthenticated devices still get filtered, even if they don’t fall into any other rulesets. AD and IP Subnet policies can then be delegated and simplified through the use of Templates, allowing you to change multiple policies at the same time.

**10. Will the date collected, either in the active system or in the reporting component, be encrypted during transmission and/or at rest?**

Typically log files are offloaded to a windows server via syslog, however the logs can also be transferred through Secure FTP and will remain encrypted on the server.

**11. Will SSL traffic have any clear text credentials stored in cache, data collection and/or reporting?**

No, our selective decryption process will not allow for passwords or any sensitive information to be stored in cache or in log files.

**12. Apple is nearing a release of their next iOS operating system for end-devices. This update is over 1gb in size, and our school districts have upwards of 5000 iPads in each district. How can your solution limit/throttle this traffic, to ensure instructional internet use can still occur, but allow end-devices to update in the background?**

iPads utilizing our Global Proxy will have full traffic shaping rules applied to them. This would allow for updates to be throttled to minimal bandwidth, but have categories such as Education still transmit at full bandwidth.

**13. Describe your data/reporting accumulator based on school, district and state level views of data.**

Provided for free with our NetSpective Content Filtering is our NetAuditor Security Event Manager. NetAuditor expands network security event management (SEM) strategies beyond basic end-point protection by accelerating the detection and automated response that leading firewall manufacturers omit in their border security offerings. NetAuditor includes automatic end-user identity association, geographic location identification by region; country; and service provider, Internet content categorization, real-time monitoring, and network event triggers.

NetAuditor is provided for ‘off-the-box’ reporting. This can install any Windows based server, VM, or desktop. NetAuditor can also report on firewall logs from many popular manufacturers for various net flow statistics.

NetAuditor’s web based administration and security management roles make it easy for ISP level customer to delegate out reporting to each school district. Districts can all access the same interface, but only run reports on their students and only run the reports that the ISP specifies, making the security event manager easier to navigate. If a district is utilizing NAT and has a local appliance, the same software can be used locally to provide further granularity into their user’s activity.