Office of Education Technology (OET)

KETS Network Services Standard

Document Owner:	Network Architect	Date Created:	7/20/2020
Approver(s):	OET Leadership	Date Approved:	10/5/2020

Summary: This document provides a standard for the configuration of systems and services that leverage the KETS network.

Purpose and Scope: This standard is intended to help districts and vendors understand the capabilities of the KETS network and the configurations that can be implemented by systems and services that run “on top” of the KETS network. They are relevant for any system or service that will be used by districts and requires TCP/IP communication between the district network and the Internet.

Reason for Implementing: A clear understanding of the configuration options available can reduce wasted effort and time and simplify implementation.

I. General

1. All devices within the KETS network (school, district, KDE, etc.) are assigned addresses from a coordinated KETS-wide Private IP (RFC 1918) range, described in the KETS Private IP Numbering Standard (available from the KETS Service Desk).
2. All connections between KETS network devices and the public Internet rely on Network Address Translation (NAT), generally configured at the district KETS firewall.
3. All devices needing to use the SIP protocol to communicate between district networks and the public Internet must support SIP ALG.
4. KETS Firewalls routinely implement Stateful Packet Inspection, Intrusion Detection/Prevention, and Port Filtering, and systems and services must be able to operate properly with these functions in place.
5. All devices connected to the KETS network should be regularly patched to correct security and other defects. Devices that cannot be regularly patched should be segmented apart and given as little access to the rest of the network as possible.
6. All devices connected to the KETS network should be identified and their impact on the network considered and monitored. District staff should have the ability to disable network access for any device that is causing issues.
7. All services that are capable of connection encryption (HTTPS and similar) should have that encryption enabled and required.

II. Inbound

1. Inbound IP traffic (from the Internet to district/school addresses) is dropped by default.

a. Districts must specifically request a public IP address and firewall entry for a device that needs to be accessible from the Internet (via the KETS Service Desk).

b. Whenever feasible, persons or systems requiring access to district devices from the Internet must use the KETS User VPN service (requested through the KETS Service Desk); examples include: staff needing remote desktop access, vendors requiring access to an HVAC management system, partners requiring access to a security camera system.

c. External systems are not permitted LDAP(S) access to Active Directory.

d. District-hosted FTP servers are strongly discouraged; SSH-based SFTP, or other alternatives such as OneDrive or Google Drive, are preferred.

III. Outbound

1. Devices assigned static IP addresses (expected to be servers, network devices, printers, and similar) can generally make outbound connections to any address.
2. Devices assigned dynamic (DHCP) IP addresses (expected to be end user devices, IP phones, mobile devices, and similar) can only make outbound connections to a relatively small number of standard ports.
    a. Districts may request additions to the allowed ports list through the KETS Service Desk.

IV. DNS

1. The district root (<*districtname*>.kyschools.us) can NOT be CNAMEd to another DNS name.
2. The namespace *.ketsds.net is for internal use only (primarily for Active Directory) and can NOT be made visible to the public Internet.

V. Digital Certificates (Private Key Infrastructure)

1. Web Server Certificates
    a. Wild-card certificates (for example, *.<*districtname*>.kyschools.us) are strongly discouraged. This would be similar to all locks in the district having one key, and multiple people having a copy of this key. It is preferred to scope the digital certificate to the specific name/use.

    b. Free LetsEncrypt certificates, using http validation, are acceptable for public sites (DNS-based validation is not currently possible). These certificates are valid for a 90-day period, so there would ideally be some automation behind this certificate.

    c. If the server is to be used only internally to KETS, internal certificates are available to be issued to these devices.

    d. Proving ownership of a domain is required before a public Certificate Authority (CA) vendor will issue a certificate. Districts should ensure the vendor can verify ownership at a subdomain level (<*districtname*>.kyschools.us), and not the top-level domain (kyschools.us).

2. Wireless Network Access (802.1x) Certificates
    a. We have an internal enterprise Public Key Infrastructure (PKI) that can issue certificates to any internal device for network access. For more details, contact the KETS Service Desk and request the Certificate Services documentation.

VI. Other

1. Membership in the Active Directory Domain Admins security group is generally not available to service accounts or district staff. District technology administrators DO have membership in a security group (Dist Support Admins) with permissions to make nearly all Active Directory user and computer management changes.
2. Service and vendor accounts in Active Directory and other systems should be given the minimum permissions necessary to function; administrative groups such as Dist Support Admins should only be used for a small number of IT administrators. The KETS Active Directory Operations Guide (available at https://education.ky.gov/districts/tech/Pages/Administration-and-Install-Guides.aspx) contains more information about Active Directory use.
3. State-wide adjustments to the configuration of the LightSpeed content filtering system are made via a request to the KETS Service Desk. Districts may add items to their own policies for permit or restrict/block but should not alter the statewide KDE PERMIT policy.
4. Adjustments to the LightSpeed SSL decryption exclude list are made by individual districts and should be requested from them.
5. Additional information about integration with the KETS environment is available from
    a. Administration and Install Guides page: https://education.ky.gov/districts/tech/Pages/Administration-and-Install-Guides.aspx
    b. KETS Product and Technical Standards page: https://education.ky.gov/districts/tech/kpur/Pages/KETS%20Technology%20Standards%20and%20Purchasing.aspx
    c. Technology Support and Services page: https://education.ky.gov/districts/tech/ksd/Pages/default.aspx

Acronyms/Abbreviations:

- OET: Office of Education Technology
- KDE: Kentucky Department of Education
- KETS: Kentucky Education Technology System
- IP: Internet Protocol
- SIP: Session Initiation Protocol
- ALG: Application Layer Gateway
- DNS: Domain Name System
- PKI: Private Key Infrastructure
- LDAP: Lightweight Directory Access Protocol
- VPN: Virtual Private Network

Related Documents:

- KETS Private IP Numbering Standard – available on request from the KETS Service Desk
- How to extend the District's Safe Computing Environment to Remote Sites (Bus WiFi) - available on request from the KETS Service Desk
- KETS Active Directory Operations Guide – available at https://education.ky.gov/districts/tech/Pages/Administration-and-Install-Guides.aspx
- Certificate Services documentation - available on request from the KETS Service Desk

Signatures

Mike Leadingham, Director of the Division of School Technology Planning and Project Management

Phil Coleman, Director of the Division of School Technology Services