Linewize
by Family Zone

TECHNICAL GUIDE

Layer 7 Visibility and Control

A guide to application and layer 7 visibility and control.

Linewize

Contents

Linewize

Introduction

In education, digital learning is skyrocketing with the proliferation of online tools, apps and affordable internet-enabled devices.

An increasing level of reliance on internet access for learning and productivity has created an expectation of high performance and easy connectivity in the classroom. At the same time, bring-your-own-device (BYOD) and cloud-computing trends have led to a proliferation in the number of devices and applications used on a daily basis. This increased use of the internet, internet-based apps, and mobile devices in the classroom bring with it several challenges for IT administrators and educators.

To ensure a high level quality service, visibility of network usage and utilisation is paramount. That, coupled with the need for educators to satisfy their duty of care toward students, introduces the need for a new type of network management. To meet these requirements, a shift away from protocol- and IP-address-based filtering is needed. A more holistic, application-aware approach to network management is required to give educators and administrators the visibility and control they need.

Linewize meets this challenge with our application-aware Layer 7 firewall. All traffic passing through the Linewize Appliance is identified using our heuristic signature- based DPI engine. This application-based identification is then harnessed to provide a high level of visibility and control.

Signature-based identification

Linewize School Manager is a cloud-managed, application-aware firewall. Application identification is first and foremost, and all traffic is matched against our heuristic signatures on a flow basis. Signatures take the form of both categories and applications. Individual flows are matched against an application, and if a individual application match cannot be made, a category match is attempted. Categories and applications form a hierarchy which lends itself to easy filtering of multiple applications while also enabling the possibility of easy granular filtering.

Signatures are maintained by Linewize School Manager and are constantly being updated for new content. Linewize Appliances download the signature database via a secure channel every 24 hours. This ensures new signatures and updates are available to the device rapidly.

Connection and flow tracking

Application identification occurs as part of the connection tracking on the Linewize Appliance. Traditionally, connection tracking has been used in stateful firewalls and routing appliances to assist with NAT of TCP and UDP connections traversing the firewall. Linewize School Manager extends this concept by performing connection tracking at the application layer. At each stage of a flow or connection, Linewize School Manager collects metadata. This can include things like HTTP hostname for HTTP packets, DNS queries/replies, HTTP Content Types, SSL certificate information and traditional TCP/IP-based transport criteria such as Ports. At a lower level, key indicators for protocols like BitTorrent, RDP and others are also collected. This metadata paints a very accurate picture of the underlying traffic type and is used to match flows against a traffic signature in real-time.

When certain types of metadata are collected, the Linewize Appliance will attempt to match all metadata for that flow against the signature database. If a match is found, this information can then be used in application and content-filtering decisions and collected for statistical purposes. Once the flow has been identified, packets matching that particular flow are marked for a fast path to reduce latency associated with the computation cost

of application-layer connection tracking. The flow has been identified so we can let it pass without further detailed inspection. This technique helps maintain network performance and facilitates line-speed application identification.

Heuristic traffic identification

Application identification in Linewize School Manager is heuristic based. Modern apps present themselves in different ways on the network and utilise different underlying technologies. From a user's perspective, there is no difference between a VOiP phone and the Facebook application they use on their computer. The difference at the networking level however is substantial. Look into the details, and you will find that VOiP traffic takes many different forms. Some VOiP products utilise standardised ports, whereas others use dynamic ports negotiated at some point in the connection setup. Still, others use standard HTTPS.

For the user, the important thing is that they can identify VOiP traffic. They need not be concerned with the underlying technology. To solve this problem, Linewize School Manager's signatures are composed of different attributes, patterns and flow behaviors that indicate that the corresponding packets match that abstract type. In many cases, more than one piece of evidence will be required for a positive match, and attributes collected may span across multiple flows to identify the connection and relationship between flows.

For a product like YouTube, this could mean that usage on a single user's machine might be composed of HTTPS traffic to youtube.com, cdn-23.youtube.com, googlevideos.com and QUIC UDP traffic to the YouTube servers. With Linewize School Manager, this traffic is all identified holistically as YouTube. This approach simplifies management of your network dramatically and paints a very accurate picture of your network utilisation.

Identification of SSL traffic

The majority of HTTP traffic now carries asymmetric SSL encryption, more commonly known as HTTPS. For many content-filtering systems, SSL encryption has been a huge issue. SSL protects the user's data by encrypting and signing the HTTPS packets at the network layer so that it is protected from eavesdropping and modification. Driven by users' desire for privacy, SSL adoption has increased exponentially and is the de facto standard for protecting data on the internet. Providing identification, visibility and filtering on traffic that is encrypted with SSL is just as important as maintaining users' privacy.

Linewize School Manager takes an approach which centers around the SNI parameter and certificate details in the initial TLS negotiation. The SNI parameter is part of the initial SSL negotiation when the client connects to the remote web server. This parameter was introduced to the TLS specification to accommodate shared load balancers and web servers that need to respond to HTTPS requests with different certificates on demand. The SNI parameter is passed by the client as the domain name, and this is identified by Linewize School Manager and matched with the signatures. This means that HTTPS traffic can be identified and matched to an application type in much the same way as regular HTTP traffic without the need for full decryption of the connection. This approach maintains users' privacy while still providing visibility and control.

Linewize

BitTorrent, VPNS and proxy servers

Peer-to-peer systems such as BitTorrent, and filtering avoidance software utilizing VPNs and proxy servers pose an especially challenging task for network administrators. These systems are specifically designed to evade filtering software and are impossible to filter and identify using traditional filtering techniques. Heuristic-based identification comes into its own with this type of traffic. Linewize School Manager uses pattern-matching techniques to identify peer-to-peer traffic, and through the collection of statistics our signatures are constantly evolving to match changing peer-to-peer networks and filtering avoidance software.

Unidentified flows and websites

The internet is a constantly evolving space. New applications and websites are launched every day, and users' browsing habits change as new tools appear in the market. It is crucial that filtering systems keep up to date with these new applications and websites on a daily basis to deal with, for example, adult content.

Periodic updates of categories simply can't keep up with the ever-changing internet. Linewize School Manager harnesses the power of machine learning to solve this problem and works with several category providers to assist with adult content identification. Unclassified website traffic originating from any Linewize Appliance is cross-checked against these suppliers, and where possible classified. This classification is done on the Linewize School Manager platform, and the results are fed directly into the signatures that all devices retrieve on a daily basis. This means new websites appearing on our platform are categorized within 24 hours and will be filtered automatically if they appear in categories that are filtered. Linewize School Manager has a team of R&D engineers that develop signatures for complex applications like YouTube, and over 90% of traffic is classified with Linewize School Manager.

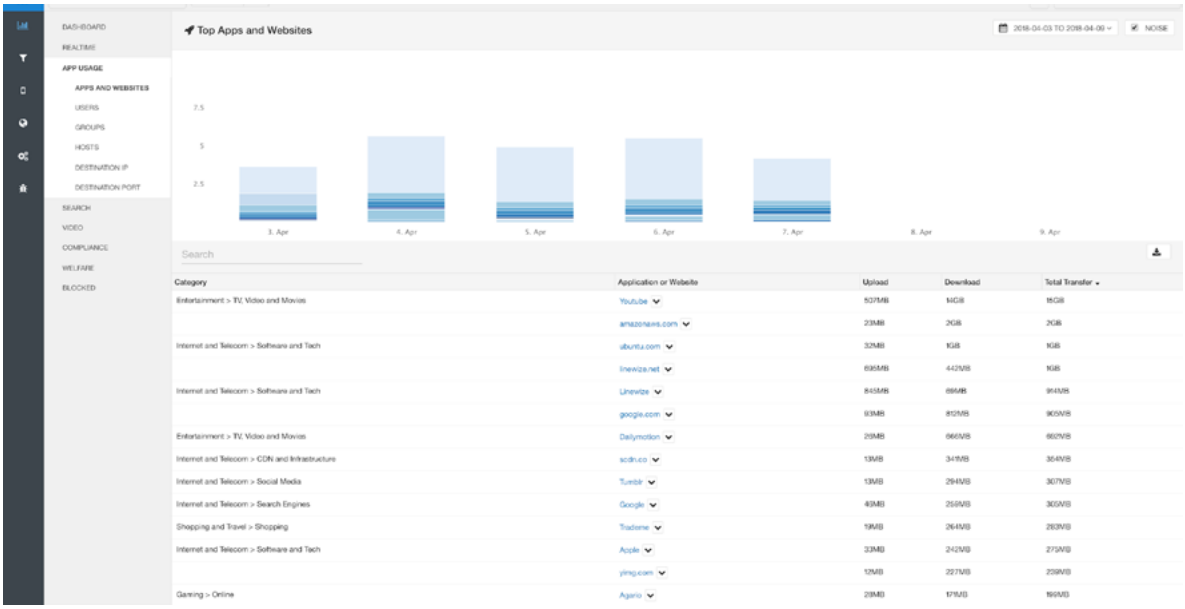
Visibility and reporting on application usage

Insight and visibility into your network is essential. With Linewize School Manager, traffic is classified into individual applications and categories. This information is pushed to our secure cloud platform, and is available in real time through the intuitive cloud dashboard. Linewize Appliances are constantly pushing metadata to the cloud platform using a highly compressed, encrypted HTTPS connection. Metadata on traffic flows is pushed in real time as flow states change and additional context information is sent on a per-flow basis, including users and applications, and the total user time spent on an application or website. Using cloud computing, Linewize School Manager then aggregates that data on an application and user basis across a customizable time period.

Traditional relational databases would take hours to deliver a query on a user or application basis. Linewize School Manager's cloud architecture is powered by a highly optimized software stack designed for elastic scalability. Instead of relying on traditional relational SQL databases, Linewize School Manager utilizes a collection of NOSQL, read-optimized and highly compressed specialised databases and aggregation engines. These systems, while powering a tremendously large data set, deliver the ability to scan and poll data within seconds, not minutes.

By utilizing this technology, Linewize School Manager can provide real-time reporting through the cloud dashboard without impacting network performance. This data provides administrators and educators with an application-centric view of their network which can be used to diagnose networking issues, locate bottlenecks and manage content access from a position of knowledge.

Linewize



Detailed breakdowns of individual applications are available through our intuitive interface right down to connection flows, and automated reports can be created within the cloud dashboard. Data is aggregated on an hourly and daily basis, which makes identifying trends and changes in network usage over time very easy. Statistics can be viewed across different dimensions to provide visibility of application usage on a user, host and group basis.

Application and content filtering

Traditional firewalls offer filtering TCP/IP criteria as well as Layer 2 criteria such as MAC address. Many content-filtering systems extend this approach to include website filtering that matches keywords in URLs for websites using regular expressions. For application content filtering, Linewize School Manager utilizes its signature-based application-layer identification system described above. Along with normal filtering criteria, such as port and IP address, with Linewize School Manager you can filter applications directly.

Filtering on application rather than port- and IP-based criteria or URL is much simpler for an administrator, and with the cloud dashboard, managing filtering policies is very easy. Rules can include time of day schedules, user and user-group membership, device fingerprint and other criteria. Application layer-filtering rules are configured from within the cloud dashboard, and separately using Linewize Classroom. From the cloud dashboard, administrators can create policies that control access to certain applications, websites and content.

A policy is much like a traditional firewall rule in that it contains certain criteria that must match for the rule to be applied. A single filtering policy could “block adult content” for all users, or “block Facebook for students during school hours.” Normally, administrators will create several rules that shape internet use and align with the internet use policy.

Linewize School Manager supports an open filtering approach that encourages good digital citizenship rather than blanket blocking and whitelisting, and our application-level filtering is geared towards this approach by providing very granular filtering capabilities.

Linewize

Blocking custom websites and content

Along with filtering content based on Linewize School Manager signatures, application-layer policies can be created to block custom signatures and websites. Administrators can create their own objects or lists that contain websites, and then utilise these in the application layer policies.

Domains are matched using a domain-specific wildcard algorithm. For example, to block stuff.com you would add "stuff.com" to an object or application-layer filtering policy. This would result in all traffic, HTTP or HTTPS, being identified by the policy. This also extends to subdomains, so requests to https://pic-cdn1.stuff.co.nz/static/pic1.png would also match. To match only a subdomain of stuff.co.nz, you would specify that subdomain. For example, to match http://cdn.stuff.co.nz you would create an object with "cdn.stuff.co.nz" as an entry. Wildcards like "htt*://stuff.co.nz/*" have no effect in Linewize School Manager and will not match.

Linewize School Manager recommends using our signatures rather than blocking websites by URL. Modern websites use a combination of CDNs and delivery networks that are often not matched by simple URL filtering.

Time, user-group and subnet/VLAN-based filtering

As with all policies in the cloud dashboard, Linewize School Manager application layer policies can be applied at specific times, can be scheduled to become active at a future date, can apply only to specific users or user groups, and can apply only to specific VLANs or subnets. This functionality is key as it enables customized filtering for different end users and devices.

Time schedules can be created by administrators in the cloud dashboard, and user and group identification ties into the identity management systems automatically.

Filtering exceptions

In many environments it is commonplace to block access to an application for all users with the exception of a select few. Linewize School Manager facilitates this need through the use of "Allow Policies." When creating application-filtering policies, Linewize School Manager offers administrators the option to allow access to a resource that was otherwise filtered by another policy.

	Allow Facebook during Lunchtime
	Allow theonionnews.com
	Block Social Media for Students
	Block Adult and Offensive Content

Application layer filtering rules

As filtering policies are evaluated in order, from top to bottom, "Allow Policies" can be placed above "Block Policies" and will allow access for specific user groups, times or network subnets. This facilitates the easy creation of more comprehensive filtering rule-sets that utilise group membership and other criteria. "Allow policies" can also be used to allow individual websites that would otherwise be blocked with another signature-based policy. This means individual websites can be cherry picked and excluded from filtering if desired.

Linewize

Alerting and reporting

Visibility over filtered content is crucial for effective network management, empowering you to educate students and users about appropriate internet usage. Filtering violations can be viewed from the cloud dashboard via emailed reporting and alerting. Filtering violations are treated with the same level of reporting granularity as normal cloud dashboard reporting. This means you can identify individual filtering violations on a user basis in real time.

Emailed alerting and reporting can also be customized to apply only to certain groups, and emailed alerts can be delivered directly in real time to the correct recipient for a specific user group.

Summary

Linewize School Manager takes a heuristic approach to application identification. Coupled with the elastic power of cloud computing and an intuitive cloud dashboard, this provides a high level of visibility and control over your network. With Linewize School Manager you get accurate, real-time data, and up-to-date user- and application-centric control.

Linewize is passionate about making student Internet management easy, and keeping students safe online on any device, any time.

About Linewize

Linewize is committed to making student Internet management easy, and keeping students safe online on any device, anywhere, any time.

Learn more

Email sales@familyzone.com
Visit us at linewize.com