family zone | EDUCATION SOLUTIONS

TECHNICAL GUIDE

Family Zone School Manager

A guide to Cloud Management of the Family Zone Appliance.

family zone | EDUCATION SOLUTIONS

Contents

Document Rev:A

Introduction

Modern networks are vast and complex. Managed Service Providers (MSPs) and IT Administrators must manage networks that may span the globe, and everyone within the organisation relies on internet access for information.

The cloud is driving an insatiable demand for faster and more reliable network access, and the pressure is constantly growing. Family Zone Education Solutions offers a novel approach to managing network access through its cloud managed, application aware firewall.

Overview

Traditional firewalls, routers and content filtering systems mostly rely on hardware appliances and local file-system based configuration. This approach, although prevalent in the networking industry, falls victim to one major flaw. In the event of hardware failure or major configuration failure, the resulting cost in engineering resource to repair the network and restore connectivity is often very expensive.

Organisations must be able to respond to a rapidly changing and increasingly demanding environment, and Family Zone Education Solution's cloud managed firewall has been built with this in mind. Cloud management provides several key advantages, and lends itself to rapid deployment, rapid recovery from issues, and appliance hardware independence.

As an MSP or IT provider with multiple sites it also provides a single secure point of control across all your networks around the globe, and contactless deployments.

Advantages of Cloud Management

The Family Zone Appliance is a cloud managed firewall, supported by a cloud dashboard. This dashboard, a browser-based user interface, adds feature-rich, elastic, and intuitive centralised management for your networks. This makes configuration remarkably simple, consistent and fail-proof.

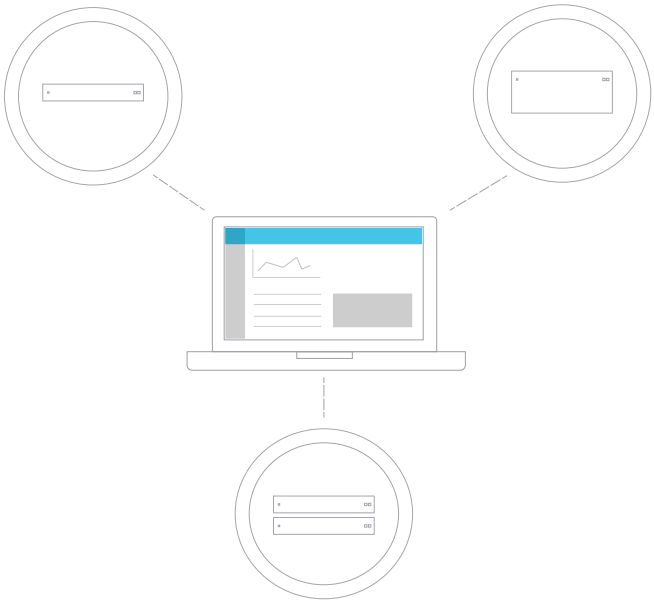
As well as simple configuration tools, the cloud dashboard utilises elastic big-data reporting tools to provide administrators with both real-time and historical insights into network use. This data provides insights that allows administrators to very quickly identify issues on their networks and provide management staff and teachers the tools to be able to manage student internet experience in a holistic way.

Simplified Deployment and Management

Before unboxing or spinning up your Family Zone Appliance or virtual machine, you can begin configuring it in the cloud dashboard. The cloud dashboard is your single pane for managing all networks.

Once powered on, your appliance will search for an internet route, connect and download configuration and any updates. If an internet route is not found, you can configure an interface manually via the command line or local web interface.

Because Family Zone School Manager is managed through the cloud dashboard, there is no need to configure complex port forwarding rules or VPNs to connect to the appliance remotely. You can have the appliance sent directly to the site and configure it remotely from day one. This allows easy reliable global management of your networks from anywhere.



Centralised Management of Networks

Easy Configuration Management

All configuration changes (apart from the base configuration on the device) are made through the cloud dashboard.

When a configuration change is made, it is stored as a change transaction. Change transactions are versioned, time stamped and associated with a particular administrator. This design means that administrators have a complete audit trail of configuration changes allowing easy diagnostics of issues created by configuration modifications. It also means reversing changes without user impact is simple and can be done remotely in the dashboard with no onsite time.

Managing the configuration in the cloud also means that in the event of hardware failure, no configuration is lost and downtime can be minimised. Replacement of an appliance is simply a matter of plugging in a replacement or deploying a new VM.

10s ago	Added web filtering rule	James
30s ago	Synced Google User Groups	James
1 hour ago	Added web filtering rule	Sam
Yesterday	Blocked Facebook for Students	Principal
Yesterday	Changed IP Address on Eth0	James

Transactional configuration management in the cloud dashboard

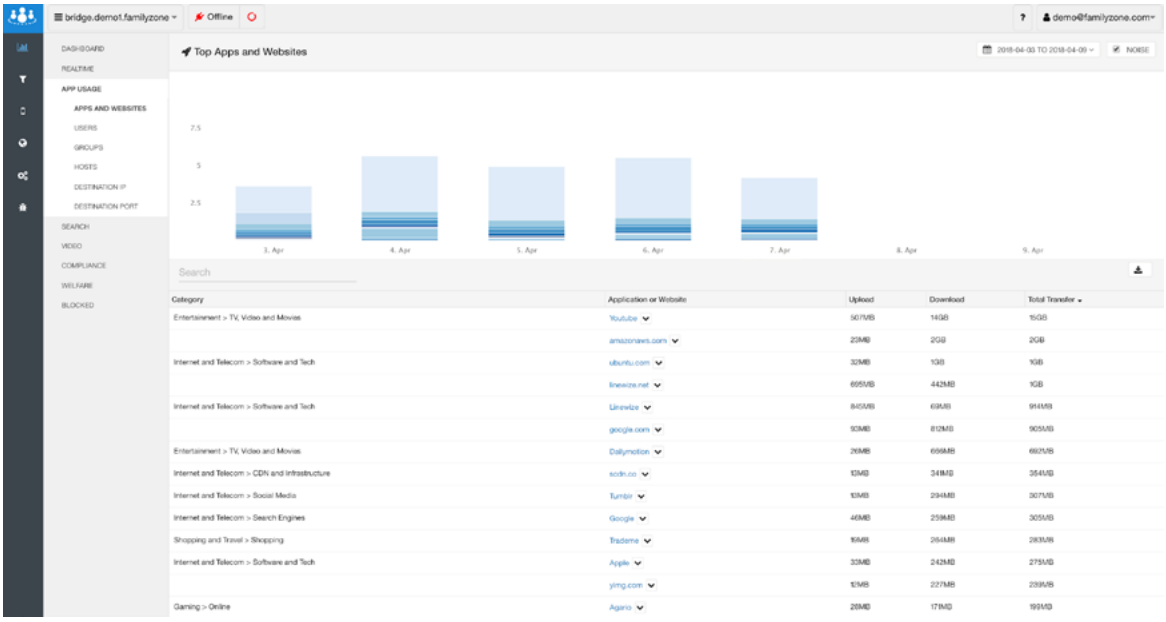
The appliance, when online, requests new configuration changes every 60 seconds and attempts to apply them. If a change cannot be applied or the device is offline, the appliance will try again and a notification will appear in the dashboard.

Reporting, Visibility and Alerting

As networks grow in size and scale, it is paramount as an administrator to have real-time visibility into how your network is performing and what your users are doing online. Family Zone Education Solutions harnesses the power of elastic cloud computing to provide detailed reporting and alerting on your network through the dashboard and other tools.

The cloud dashboard provides real-time visibility into application usage, transfer rates, client connections, malware, DOS attacks and filtering hits in a easy, intuitive drill-down interface.

All statistics are live, and it retains 3 months of data for historical reporting. Emailed reports can be created from data in the cloud dashboard, and alerts on both usage and errors can be easily configured so you are on top of any network issues that arise.



Realtime reporting on application usage

Statistical metadata is pushed to the cloud platform via industry standard HTTPS with TLS with a maximum delay of 5 minutes. As with the configuration, the appliance does not store any reporting data.

Because reporting is not managed by the appliance itself, resources are not wasted processing reports on the appliance thus improving network throughput dramatically. Logs, coredumps and error reports are also updated in real-time to the cloud platform. This means that even if the appliance is offline, diagnostic data can still be retrieved.

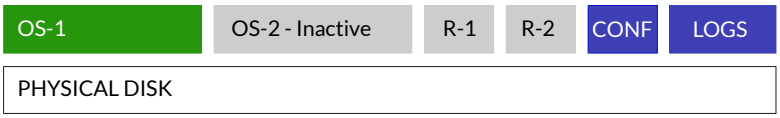
Automatic Managed Updates

Updates are a common problem with network firewalls and other network appliances. They are seldomly applied, as they risk downtime and often break functionality.

As a result of this, security holes and bugs go unpatched often for the life of a product which puts networks at serious risk of security breaches and performance issues.

Family Zone Education Solutions believes in rapid software development and provides mandatory automatic updates. Updates are applied automatically and in a transactional fashion. If an update fails to apply or contains a bug, your appliance will rollback to the previous state automatically. This is achieved through the use of an Active/Inactive OS partitioning scheme on the disk. Updates are downloaded, checked for validity and then written to the inactive partition. When all checks have been successful and the image is validated, the appliance will reboot and attempt to boot into the new update. If anything fails during boot or the appliance cannot resume connection with the cloud, it will reboot and try again. If it fails to boot twice then the appliance will rollback to the previous state.

This approach prevents down-time due to software bugs and enables us to rapidly respond to feature requests, security issues and bugs transparently and without major downtime.



Disk partitioning in SphireOS for rapid transactional updates

Working with the Cloud Managed Firewall

How the appliance connects to the Family Zone School Manager

Configured in every Family Zone Appliance is a device-id, region and key. Family Zone operates several isolated datacenter regions in different countries.

Along with the region identifier, the device-id and key provide the basis for identification of the appliance, configuration, reporting and the real-time cloud connection.

Cloud connection details

If you have a physical appliance, the device-id and key will have already been configured in your appliance. If you are creating a Virtualized Appliance, then you will need to create these credentials in the Cloud Dashboard.

Your device-id is unique for your particular network rather than a particular piece of hardware. This is important to remember if you need to replace your appliance - simply use the same device-id and key in the new appliance. All configuration in the cloud dashboard is tied to this identity.

During boot, your appliance attempts to connect to the internet, then makes several connections to the Cloud Platform in the configured region to retrieve configuration, application information and push reporting information.

Power on	System is powered on, the boot manager selects the active OS partition.
System initialised	System begins initialising components and processes.
Base configuration loaded	The base configuration is loaded from the filesystem. This includes the cloud credentials and basic networking configuration.
Device enters degraded state	Device enters the degraded state. Until all configuration is loaded from the cloud, the device will not allow internet traffic through.
Load configuration	Device tests for an internet connection and connects to the configuration gateway. Once connected it attempts to load the latest configuration revisions.
Load signatures	Device loads the signatures from the appindex.
Realtime connection	Establishes a connection with the scloud-xlb nodes. This connection will be used for user authentication, realtime metrics and other non-configuration based API calls.
Devices leaves degraded state	Device leaves the degraded state.
System operational	Everything is running, internet traffic will be allowed and normal filtering is operational.

During boot and normal operation there are several remote assets that are required.

Server	Port/Protocol	Purpose
scloud-xlb.<region>.linewize.net	TCP/443	Realtime management connections
stats-xlb.<region>.linewize.net	TCP/443	Statistics and reporting metadata
collector-xlb.<region>.linewize.net	TCP/443	Logs, coredumps and diagnostics
ping.linewize.net	TCP/443/ICMP	Watchdog monitoring
8.8.8.8	UDP/53	Internal DNS lookups
configuration-gw.<region>.linewize.net	TCP/443	Configuration retrieval
sphireos-updates.<region>.linewize.net	TCP/443	Update notifications
s3-ap-southeast-2.amazonaws.com	TCP/80/443	Update images

Some content filtering systems block access to certain resources. Although not normally required, it is important to add these domains as exceptions to any content filtering system that are operating on your network.

What Happens if the Internet Connection is Offline

If the internet is unavailable during boot, or the appliance is unable to retrieve the configuration from the cloud platform, the appliance will stay in the degraded state.

This means administrators will be able to access the appliance locally to diagnose the issue, but users will not be able to browse the internet, and changes made in the cloud dashboard will not take effect until the appliance has reconnected. This approach is crucial as, without configuration, users may be able to browse the internet freely without filtering.

If the internet connection is interrupted after boot, during normal network operation, the Family Zone Appliance will continue to operate unimpeded. Filtering will still be applied to users on the network and all configuration will be maintained in memory. Configuration changes that are applied in the cloud dashboard will not take effect until the internet connection is restored.

Local Management Access

When working with cloud managed appliances, a 'chicken-and-egg' situation can sometimes occur during initial configuration or maintenance.

A connection to the internet is required for management of the Family Zone Appliance which in some situations is not possible. To solve this problem, Family Zone has built a local Command Line Interface (CLI) and web based tool that can be accessed without an internet connection.

These tools provide administrators with the ability to configure the network interfaces and routing along with the device-id, region and key.

If you are installing Family Zone School Manager in a virtualised environment, you will need to use these tools to perform the base configuration and connect your appliance to the cloud. Along with base configuration, the local management tools also provide some basic diagnostic tools such as ping, traceroute, dig and a packet capture facility. These tools will help in diagnosing issues when your internet connection is down.

The CLI requires console access which is enabled by default on all Family Zone Appliances.

Method	Command	Description
Serial	Baud, 115200,8n1	Direct console access via a serial cable
Screen/keyboard	---	Direct console access
SSH	ssh admin@192.168.1.1 -p 5022	SSH access on port 5022. Default password is “admin” or the device key
Web console	https://192.168.1.1:5001	Default password if “admin” or the device key

If you are configuring the device for the first time the key will be “admin”, otherwise you can find this key in the cloud management interface and via the serial console. The username for accessing management accounts is always “admin”

Summary

Family Zone Education Solution’s cloud managed firewall has been built from the ground up to offer a more reliable, secure and simpler networking experience. Our cloud platform is constantly evolving, and is built on industry tried and tested technologies to ensure a high level of resiliency and reliability.

Family Zone Education Solutions is passionate about making student internet management easy.

About Family Zone Education Solutions

Family Zone Education Solutions 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 familyzoneschools.com