



Design and Implementation of a Content Filtering Firewall Proposal

Version:	1.3
Date:	14 March 2019
Submitted to:	ICT (MR.NIYAS)
Organization:	UNITED FOOD SUPPLY PVT LTD

Product Used



Organization



Proposed and Install By.



Document History

Version	Summary of Changes	Date
1.0	Proj't requirements with preliminary info	03/09/2020
1.1	Further information collected	03/14/2020
1.2	Preliminary physical site survey "done"	-----
1.3	First draft proposal is prepared	03/14/2020
1.4	Revised copy of proposal with client's ICT	
1.5	Final proposal is prepared	
1.6	Implementation report	

Considerations by the client's Technical team

Date	Consideration
03/09/2020	<p>Request passed by the ICT team; Scalable and affordable Internet management solution that is easy to Manage and cheap to upgrade. The main objectives are Boost WAN Speed & Manage Bandwidth Costs</p> <p>Solution desired;</p> <ul style="list-style-type: none">• Manage Bandwidth & Control, Captive Portal• Web and Content Filter• Anti-virus, Anti-spyware, Spam Blocking• WAN Failover, WAN Balancer, OpenVPN• Application Controller, Ad Blocker

Purpose of document

This document defines the "Untangle: Network Security for SMB".

Untangle takes the complexity out of network security—saving you time, money and frustration.

Get everything you need in a single, modular platform that fits the evolving needs of your organization without the headaches of multiple point solutions

Background

A firewall is a system for enforcing access control policy between two networks and is one of the most important measures to protect against network attacks. Firewalls traditionally protect the internal network from outside threats. But there has been increasing need for preventing the misuses of the network by the internal users which most previous firewalls overlook. In this paper, we propose a method of adding content filtering functionality to the firewall and describe its implementation. We also show a new attack that combines JAVA Applet and XML to get around the content filtering firewall, hence showing the need for clear usage policy for software and systems

Objectives of the project

The primary objective of the project is to supply and install Scalable and affordable Internet management solution

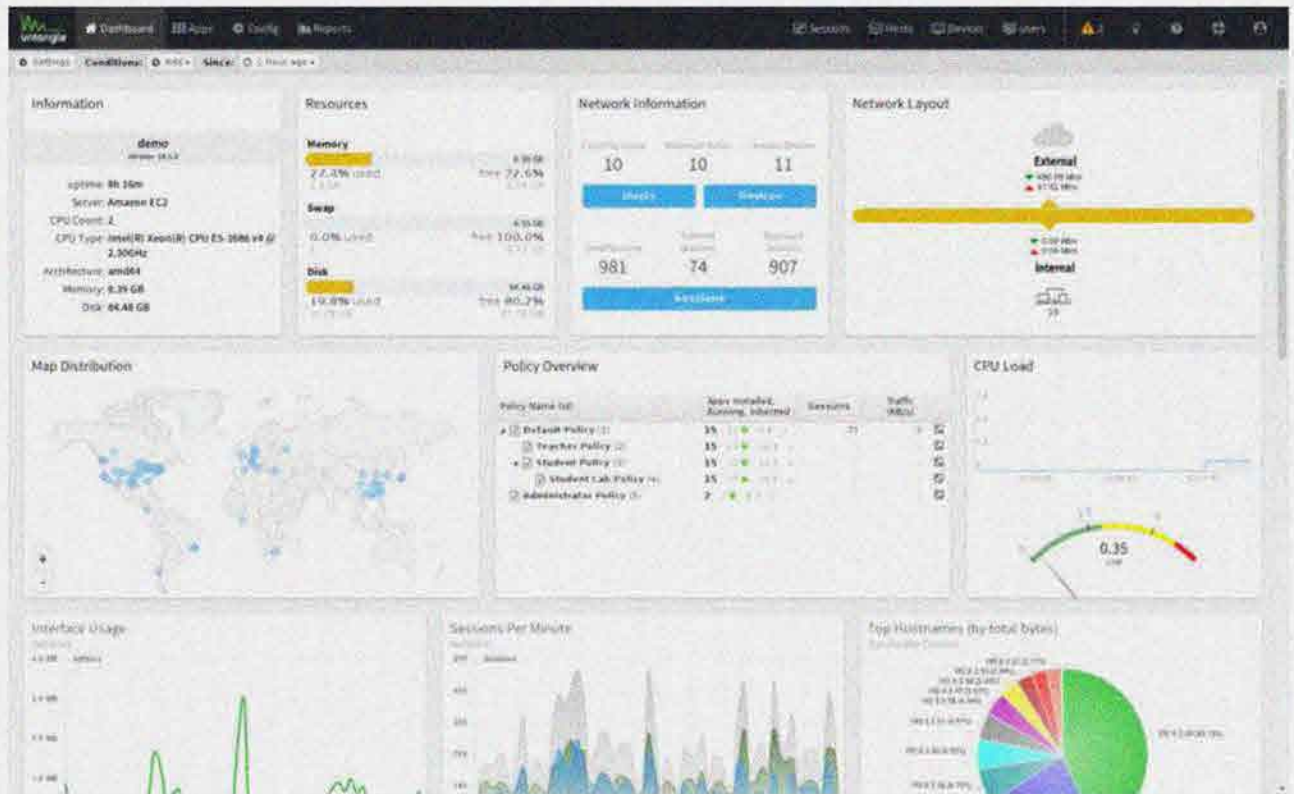
- Manage Bandwidth & Control, Captive Portal
- Web and Content Filter
- Anti-virus, Anti-spyware, Spam Blocking
- WAN Failover, WAN Balancer, OpenVPN
- Application Controller, Ad Blocker

Untangle NG Firewall

Untangle NG Firewall is a Debian-based network gateway with pluggable modules for network applications like spam blocking, web filtering, anti-virus, anti-spyware, intrusion prevention, VPN, SSL VPN, firewall, and more.

Dashboard

The Dashboard provides an overview of the state of your NG Firewall. It is extremely useful for quickly viewing or monitoring what is happening on the network and the current status of the Untangle server.

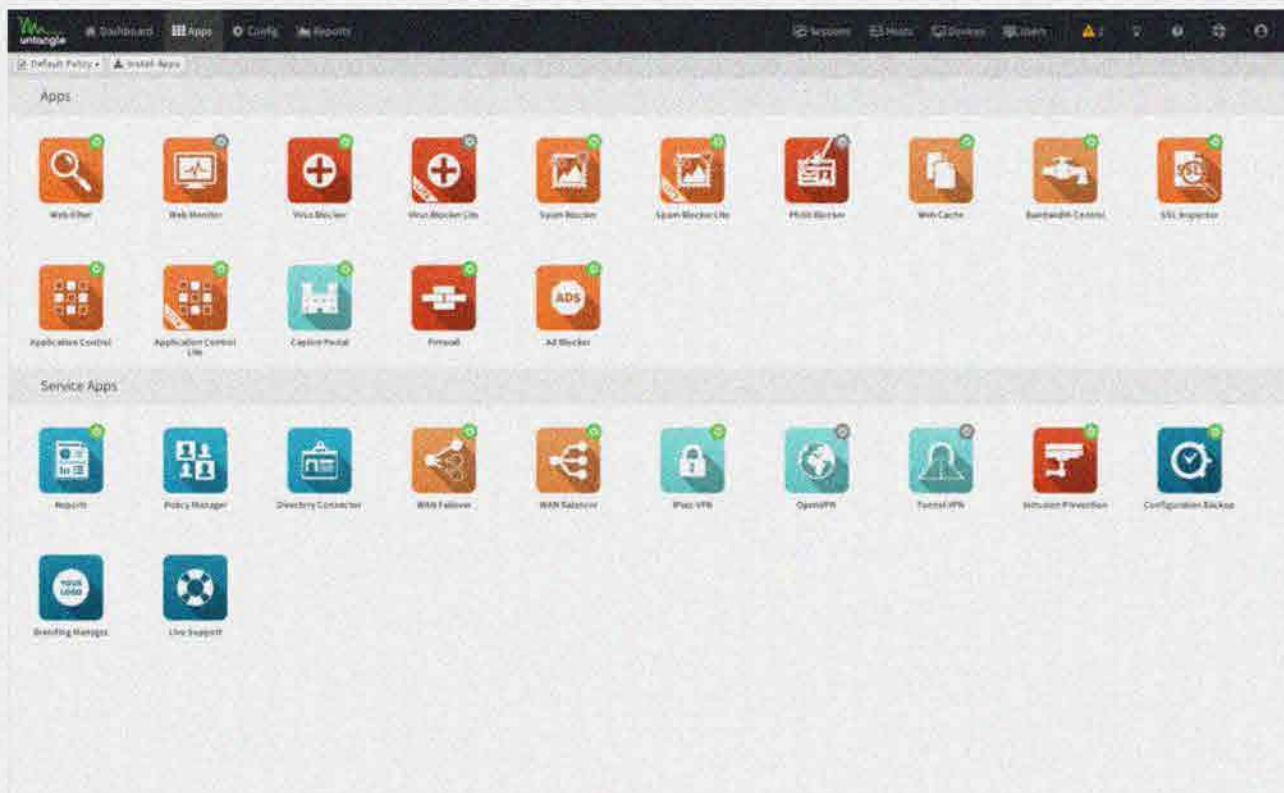


By default, the dashboard will show several widgets with varying pieces of information. However, the dashboard is completely customizable. Widgets can be removed and added so the administrator sees exactly the information that is important to them on the dashboard.

Applications

Applications are little plugins that add functionality to your Untangle server - just like "apps" on an iPhone or Android device.

On the Apps tab you'll see the currently installed apps. Across the top there is a dropdown menu to switch to different Policies. Policies can be controlled via the Policy Manager app.



Apps can be installed by clicking the "Install Apps" button at the top. It will display the apps that can currently be installed. To install an app simply click on its icon. You can install as many apps at the same time as you like. After starting the installation of the desired apps you can click the "Done" button at the top to go back to the apps view.

Once installed the applications' settings can be configured by clicking on the Settings button or the icon of app, depending on the skin. Applications install with the suggested configuration which is the default settings and on/enabled in most cases. An application that is off/disabled will not process any network traffic. To enable a disabled application, edit the settings and click "Enable" on the first tab inside the settings.

Bandwidth Control

Bandwidth Control gives you the power to monitor and control bandwidth usage on your network. It can be used to ensure that your network continues to operate smoothly and that bandwidth is shared optimally based on what is important to you. Many organizations struggle with bandwidth problems such as students watching online videos or clients using BitTorrent while more important tasks struggle to complete for bandwidth. You can use Bandwidth Control to do things like give high priority to Video Chat or slow down all traffic coming out of machines using BitTorrent.

Web Filter

Web Filter monitors HTTP and HTTPS traffic on your network to filter and log web activities and block inappropriate content. Web Filter also appeals to customers who require an added level of protection or are subject to regulations, for example Web Filter helps libraries comply with the [Children's Internet Protection Act](#)). Need to block Pornography or Hate Speech on your network? Web Filter is your answer.

Virus Blocker

Virus Blocker transparently scans your HTTP, FTP and SMTP traffic to protect your network from viruses, trojans and other malware. It scans within archives such as zip, rar, tar, gzip, bzip2 (and more).

As files are downloaded onto the network Virus Blocker scans downloads using many technologies. Firstly, it will collect metadata about the file and query the Untangle threat intelligence database for information about the file based on its fingerprint. Secondly, a local scan using Bitdefender's signature database will be run on the server while the cloud lookup is being performed. Thirdly, a heuristic scan is performed to look for suspicious patterns in executable files. Lastly, dynamic analysis is performed by evaluating code in an emulator and looking for malicious activity. If the download fails any of the above test it is considered malware and the download is blocked

Spam Blocker

Spam Blocker is an intelligent email filter that identifies and handles spam (unsolicited bulk email). It leverages technology from the Spam Assassin project and improves upon it with the integration of a commercial spam engine. It can scan any email that is transported via SMTP.

Spam Blocker transparently scans email transported over SMTP on the way to your mail server (or outbound if configured so). It does not require any reconfiguration of your DNS MX records or the email server. Any SMTP traffic going through the Untangle server will be scanned.

WAN Failover

WAN Failover works in conjunction with multiple ISPs to assure that you maintain Internet connectivity if a loss of connectivity occurs on one of your WAN connections. If one of your ISP links goes down, WAN Failover will automatically route all traffic over the other WAN(s) until service is restored.

You may also consider using WAN Balancer in your network as well - it allows you to maintain an automatic distribution of traffic over multiple WAN links rather than just failing over if one goes down.

Tests are configured for each WAN which are run continuously to determine the current status of each interface. If enough test fail on a given WAN to exceed the failure threshold then the WAN is considered down and internet-bound traffic will not go out that WAN. The lowest ID active WAN is used as the current default WAN interface for internet-bound traffic.

Application Control

Application Control leverages the Network Application Visibility Library (NAVL) from ProCera Networks to perform deep packet (DPI) and deep flow (DFI) inspection of network traffic. This allows the server to accurately identify thousands of today's common applications such as Social Networking, P2P, Instant Messaging, Video Streaming, File Sharing, Enterprise Applications, Web 2.0 and much more. For most common applications you can simply go the list on the Applications tab, check **Block** for anything you want to stop, then Application Control will take care of the rest. If you need a higher degree of control you can use the Rules tab to create custom rules which target more complex traffic patterns.

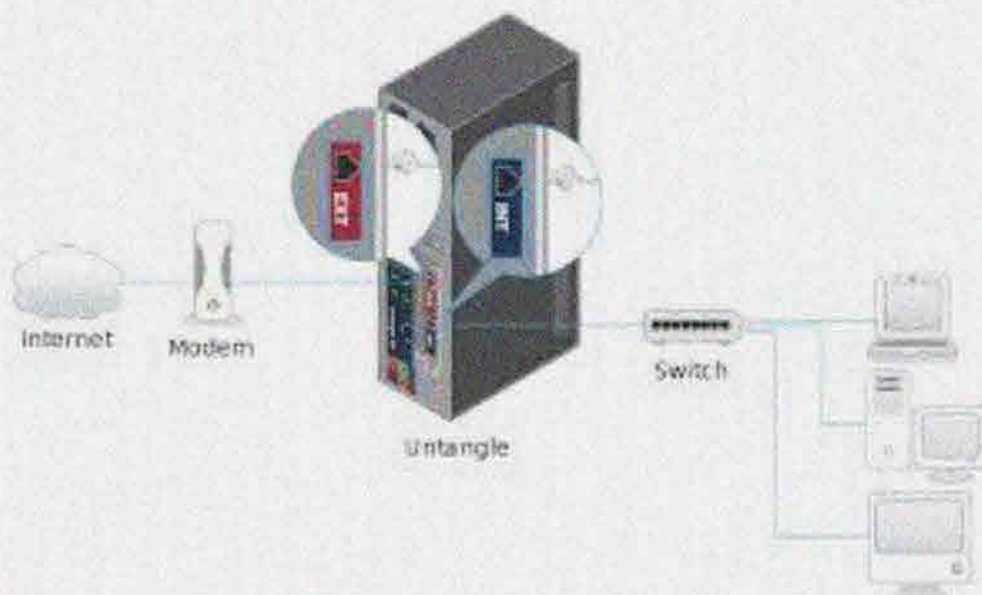
Using your own Hardware

One of the great things about Untangle is that we're software based, meaning you can install it to any desktop or server PC that fits the bill. When putting together an Untangle server you must account for several variables - the hardware you're installing onto, the number of users as well as the workload of those users. The table below provides some recommended hardware specs by network size.

Hardware Recommendations Table

Resource	Processor	Memory	Hard Drive	NICs	Notes
1-50 devices	Atom/P4 equivalent or greater	2 GB	80 GB	2 or more	
51-150 devices	Dual Core	2 or more GB	160 GB	2 or more	
151-500 devices	2 or more Cores	2 or more GB	500+ GB	2 or more	
501-1500 devices	4 Cores	4 or more GB	500+ GB	2 or more	64-bit
1501-5000 devices	4 or more Cores	4 or more GB	500+ GB	2 or more	64-bit

NG Firewall Installation



Financial consideration

Untangle's network solutions are simple and powerful, and we believe that buying them should be just as straightforward. You can customize a solution to fit your needs, the complete your purchase online. We're standing by to help if you need assistance.

Option 01

Licensed Devices Up to 25

License Term: Annual 10% Discount

Hardware: Our own Hardware (Customer Need to Provide)

NG Firewall Complete **Price \$540.00**

Product	Configuration	Quantity	Total
NG Firewall Complete	Licensed Devices: [?] Up To 25 License Term: Annual (10% Savings)	1	NG Firewall Complete 1-Year Subscription Up To 25 \$540.00
	Support & Services:		
	Branding Manager: [?] Included		Command Center
	Live Support: [?] Included		Included
	<input type="checkbox"/> Conversion Service [?]		
	<input type="checkbox"/> System Installation & Configuration [?]		
	<input type="checkbox"/> System Optimization Service [?]		
	[?] Required fields		Price: \$540.00

Option 02 (Recommending)

Licensed Devices Up to 50

License Term: Annual 10% Discount

Hardware: Our own Hardware (Customer Need to Provide)

NG Firewall Complete **Price \$1,080.00**

Product	Configuration	Quantity	Total
NG Firewall Complete	Licensed Devices: [?] Up To 50 License Term: Annual (10% Savings)	1	NG Firewall Complete 1-Year Subscription Up To 50 \$1,080.00
	Support & Services:		
	Branding Manager: [?] Included		Command Center
	Live Support: [?] Included		Included
	<input type="checkbox"/> Conversion Service [?]		
	<input type="checkbox"/> System Installation & Configuration [?]		
	<input type="checkbox"/> System Optimization Service [?]		
	[?] Required fields		Price: \$1,080.00