Project:

Implementation of Cloud-based Parental Control (CPC) on an Embedded Wireless Router

NetGenie is a Wi-Fi product for Homes implementing Parental controls with respect to Internet usage in families. The project involved porting of their existing Parental Control Software on Embedded System of Net Genie. Salient features of NetGenie Parental Control include the following:

1. Identity-based Network access
2. Content control – blocking offensive and inappropriate sites for children
3. Image and pop-up blocking - Prevents display of adult content and advertisements
4. Customized usage per age group – Customized access privileges for each member of the family in accordance with their age and online content preferences
5. IP address black list
6. MAC address white list

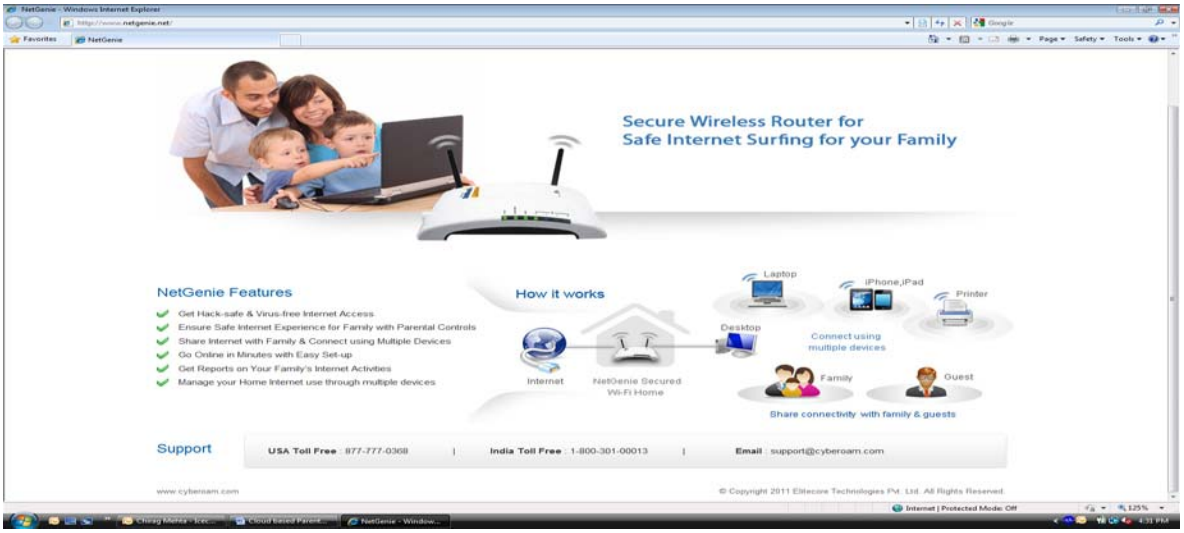
With a user-friendly web interface, NetGenie allows the administrator (one member of any family) to monitor the web and mail activity for each family member with a detailed account of sites visited and total time spent online along with attempts to visit blocked sites and applications. A password authentication system for the administrator prevents unauthorized users from disabling Internet surfing policies.

Introduction – Net Genie

Net Genie Parental Control ensures a safe Internet experience for the entire family. It empowers parents to balance the online environment for children by prohibiting access to unsafe sites like pornography as well as regulate access to entertainment, gaming and other recreational sites. The objective is to allow parents to enforce learning component into the online activities of children where they are forced to earn gaming/entertainment time while working through educational contents.

With a security component consisting of firewall, intrusion prevention and anti-virus, NetGenie parental control keeps hackers, viruses and other intruders at bay when the family surfs the web. NetGenie protect children from harmful Internet content while managing their Internet time and experience with its Parental Controls feature. Administrators can also get reports on home Internet use along with family's Internet activities to manage NetGenie configuration – through any Internet-access device at the home.

NetGenie enables a secure Wi-Fi home where family members can access Internet from any corner of the house. NetGenie offers Internet access using various devices like computers, laptops, PDAs, smart phones, iPADs and more! Apart from sharing Internet connectivity with family members, it also connects Internet-enabled devices like printer, gaming consoles and more across the home.



Secure Wireless Router for
Safe Internet Surfing for your Family

NetGenie Features

- ✓ Get Hack-safe & Virus-free Internet Access
- ✓ Ensure Safe Internet Experience for Family with Parental Controls
- ✓ Share Internet with Family & Connect using Multiple Devices
- ✓ Go Online in Minutes with Easy Set-up
- ✓ Get Reports on Your Family's Internet Activities
- ✓ Manage your Home Internet use through multiple devices

How it works
Internet
NetGenie Secured Wi-Fi Home
Laptop
iPhone,iPad
Printer
Desktop
Connect using multiple devices
Family
Guest
Share connectivity with family & guests

Support | USA Toll Free : 877-777-0368 | India Toll Free : 1-800-301-00013 | Email : support@cyberoam.com

www.cyberoam.com © Copyright 2011 Elitecore Technologies Pvt. Ltd. All Rights Reserved.

Challenges in Embedded Environment

The embedded environment presents unusual challenges to the coder. These systems are characterized by small memories, aggressive and idiosyncratic microprocessors, performance sensitive applications, and real-time applications. All too often, the available compilers fail to satisfy either the space or performance requirements, and the user must program at least part of the system in assembly code.

To address these challenges, NetGenie has adopted various methods including data compression which greatly increases the memory in the embedded system while ensuring they don't get slowed down. It has also trimmed down application size and memories to create a buffer so that the system does not get slowed down when under heavy use.

Programmed in this way, NetGenie can use far less memory to run various applications in the GUI, icons and menus, policy setting and more, whose compressed sound and image data are normally expanded when they are in RAM.

Parental Control Function in Net Genie

NetGenie allows parents to select age-appropriate Internet access that allows kids to access websites and web categories that are deemed safe for their age group. At the same time, it blocks inappropriate websites, content and images. NetGenie allows the user to be as specific as he/she wants – adding more sites to be blocked or creating exceptions to the existing list of blocked sites to meet specific requirements. One can also control access to applications like games, social networks, instant messengers, file transfer and more.

What is Cloud based Parental Control?

To understand what is cloud based parental control, let us understand prevalent different types of parental controls in Embedded Routers.

A) Parental Control using black list : In this type one can achieve limited control as the black list updating has to be carried out on a regular basis, however, there is high risk of 'bad sites' sneaking through.

B) Parental Control using White list: In this type, a list of websites in prepared which is accessible and all other websites are blocked. There is a high maintenance cost and it gets difficult to maintain as the size of the white list increases

C) Parental Control using DNS: This is the best of all the above mentioned, but this is domain based and hence it does not take URL into consideration For example: www.nytimes.com/sports is a different category then www.nytimes.com/finance

There is a new method of Parental control, which is Cloud based parental control, which addresses the shortcomings of prevalent methods.

Cloud-based Parental Control: How it works in NetGenie

Cyberoam NetGenie's Cloud-based parental control (CPC) mechanism addresses the shortcomings of existing parental control solutions by extending real-time protection to the Cloud, with granular restrictions that limit not only the types and categories of site information and applications that children can access online, but also when they can access it.

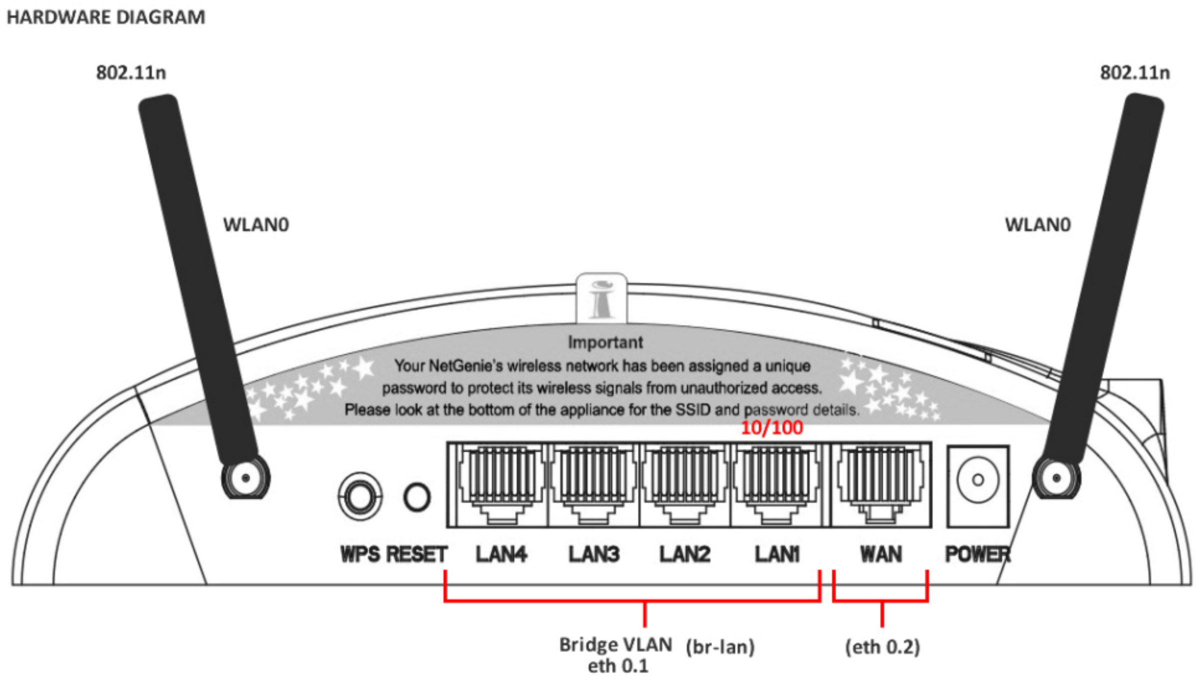

HARDWARE DIAGRAM
802.11n
802.11n
WLAN0
WLAN0
Important
Your NetGenie's wireless network has been assigned a unique password to protect its wireless signals from unauthorized access. Please look at the bottom of the appliance for the SSID and password details.
10/100
WPS RESET
LAN4
LAN3
LAN2
LAN1
WAN
POWER
Bridge VLAN (br-lan)
eth 0.1
(eth 0.2)

Figure 1: NetGenie hardware diagram

Quick and easy to set up, NetGenie is a simple plug-and-surf appliance, resembling a Wi-Fi router. It allows seamless connectivity through various devices including computers, PDAs, smartphones and iPads. For effective parental controls, NetGenie has a GUI which allows the configuration of age group-appropriate Internet access for children and other family members, thereby eliminating the need to physically monitor their online activities.

Architecture of Netgenie:

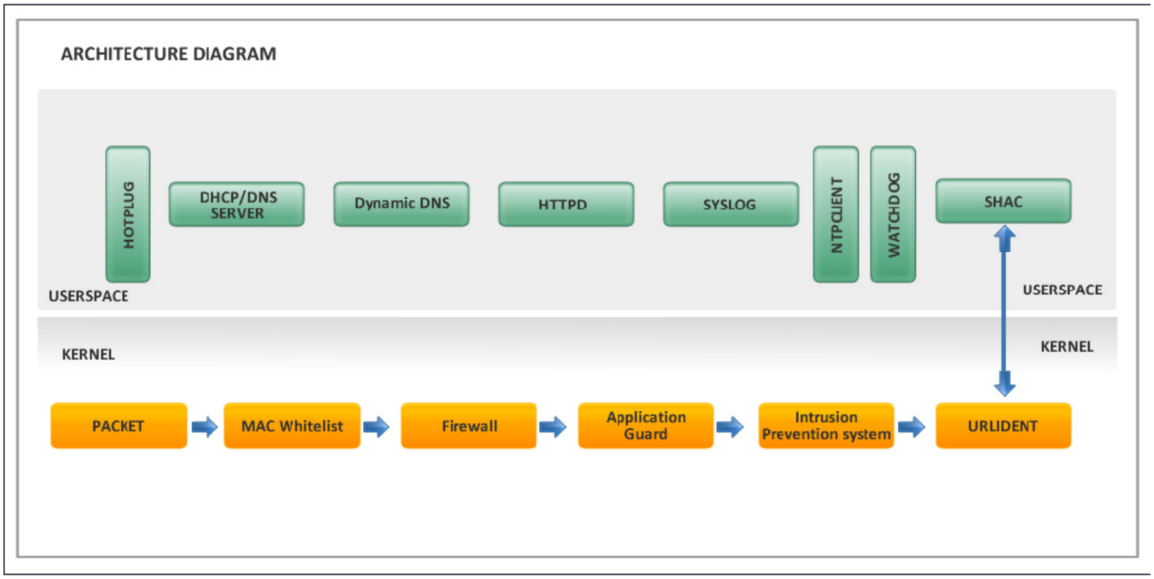


Figure 2: Architecture of NetGenie with modules in detail

Just like conventional computer operating systems, NetGenie's virtual memory can be divided into a kernel area and user space, the latter is where all user mode applications for NetGenie are running to enforce parental controls.

For data transfer over the internet from LAN to WAN (as depicted in fig.2), any outgoing data packets flow through the directed scheme in kernel as shown in the diagram. The flow of packets is directed by means of an "intelligent pattern matching engine" which is an authorization engine designed for easy and efficient management of access rights for various users in the family including children.

1. The data packets are initially analyzed by a "MAC white list" consisting of MAC addresses of allowed web access devices. This white list of allowed devices can be set up in advance by the administrator using the NetGenie GUI.

2. NetGenie now filters the data to the local firewall which is designed to protect the internal LAN from DOS, DDoS and IP spoofing attacks while tracing the data packets to prearranged home users who can be identified by NetGenie through their username and password.

3. After this, the local Application Guard comes into picture. Its task is to manage access rights to various web applications by comparing and validating signatures.

4. The local Intrusion Prevention System with enhanced signatures database, gives an additional layer of protection from application-level attacks, intrusion attempts, malware, Trojans, backdoor activity and other malicious threats.

5. NetGenie has an in-built Secure Home Appliance Client (SHAC) which communicates with the Cloud. The Cloud-residing "URLIdent" within shad is tasked with directing communication flow on HTTP between the local and remote sockets, tracing the data to a pre-assigned website categorization engine called "WebCat", which allows or blocks access for various users to various website categories such as "Chat", "Games", "Social Networking" and more.

6. Among other support functions of SHAC, the "watchdog" keeps track of whole system for connectivity status, the "NTPClient" keeps track of time, "Syslog" gives logs and reports on network activity, "HTTPD" runs the NetGenie GUI, "Dynamic DNS" gives DNS updates for IP, the "DHCP/DNS server" is assigned to solve DNS resolution queries and lease IP addresses over DHCP.

7. Finally, the "hotplug" is used to dynamically adapt to system configuration changes. It is also used by the kernel to notify user mode software when some significant (usually hardware-related) events take place.

Modules and Workflow in detail

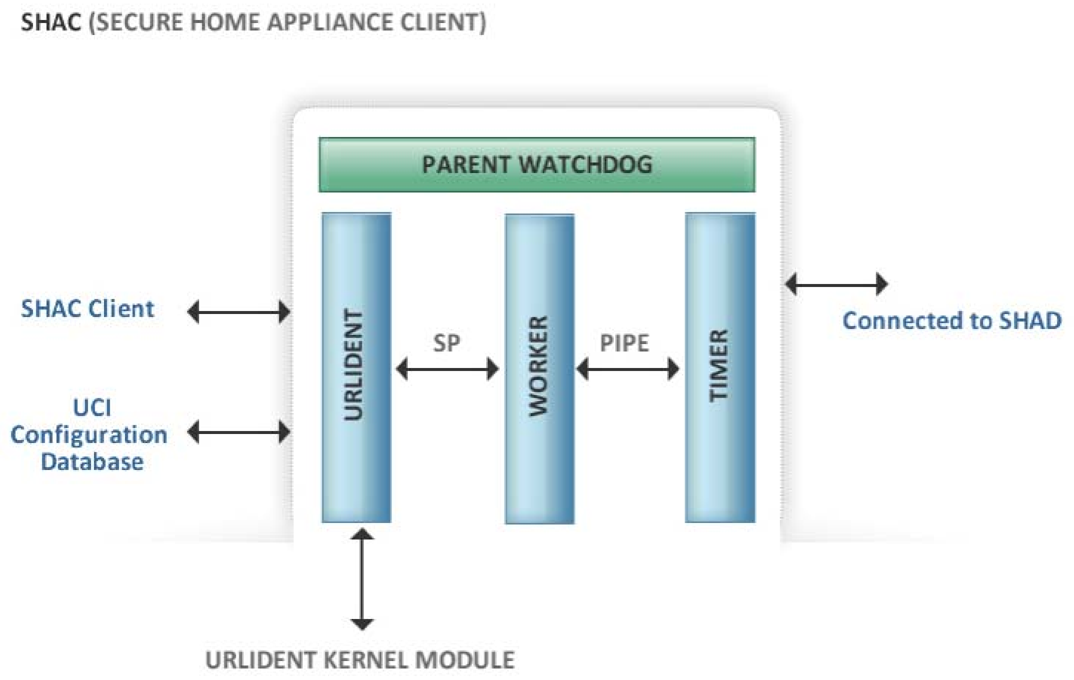
A brief description of various NetGenie modules has been covered in previous section. To understand the parental controls workflow in detail, refer figure 3. As shown earlier, the SHAC daemon which continuously works on the NetGenie system, is assigned the task of communicating with the Cloud, looking up various URLs to find ones which may be allowed or blocked based on various definitions.

1. To enable SHAC, there are three internal processes: the WORKER, the TIMER and the URLIDENT.

2. The URLIdent process reads various URLs from the kernel, directs communication flow between the local and remote sockets, thus allowing or blocking access to various sites for various users as per various access control lists.

3. The Worker process is assigned the task of sending and receiving URLs between NetGenie and the external Cloud.

4. The timer maintains policies and access control rules.



THREE PARTS:

WORKER : sends & received URLs SHAD Listens on UNIX Port

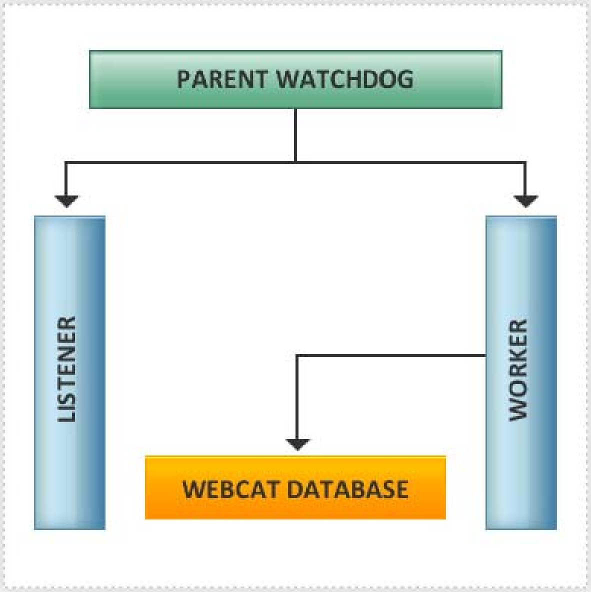
TIMER : Maintains Policies & ACLS

URLIDENT : Read URLs from Kernel

Figure 3: NetGenie workflow in detail

As shown in Figure 4, the Cloud-residing SHAC daemon is assisted by a “Parent watchdog” which is assigned the task of listening for connection on TCP Port 197, 443 and 53 and coordinating with URL categories list, “Webcat”. It also serves firmware updates.

SHAC (SECURE HOME APPLIANCE DAEMON)



Located on Cloud

Listen for Connection on TCP Port 197, 443, 53

Serves Webcat Queries

Serves Firmware updates

Figure 4: SHAC in detail