THE OPEN SOURCE NETWORK SECURITY SOLUTIONS

Author:

Jegan Srimohanram

Mobile : +91-9790239061

Email ID : opensourcejegan@gmail.com

www.linkedin.com/in/jegansrimohanram

Goto Index

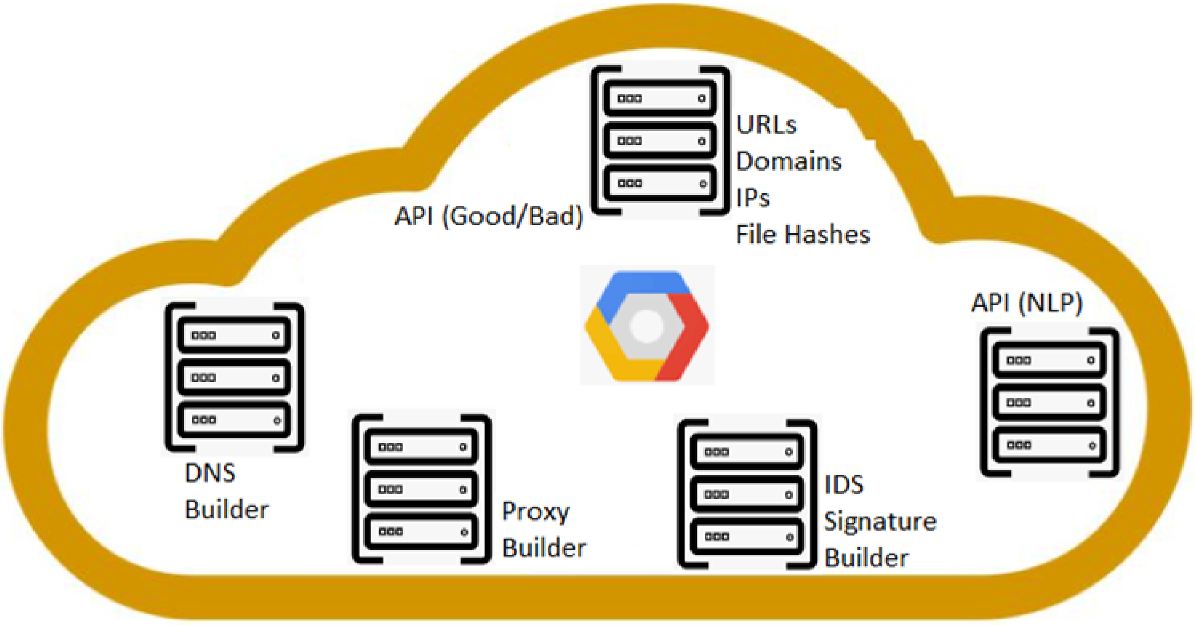
INDEX

Goto Index

Product Objective:

Using the **Vulnerable Internet parameters like URL,Domain,IP address,File Hashes,Packet Headers/Payload** , a **public cloud infrastructure** is built in the form of API to provide Good/Bad responses , such that Secure IT infrastructure components like DNS Server,Proxy Server,Browser Extensions/AddOns,Antivirus,Intrusion Detection System (IDS) and Layer 3 Swtiches can **Allow or Deny** a user/endpoint/server request accordingly.

Our Public Cloud Infrastructure:



API (Good/Bad):

Using the Vulnerable Internet parameters like URL, Domain, IP address, File Hashes, Packet Headers/Payload , a public cloud infrastructure is built in the form of API to provide Good/Bad responses , such that Secure IT infrastructure components like DNS Server, Proxy Server, Browser Extensions/AddOns, Antivirus, Intrusion Detection System (IDS) and Layer 3 Swtiches can Allow or Deny a user/endpoint/server request accordingly.

API (NLP – Natural Language Processing)

Using a specific AI-ML model in an API we predict URL / Domain categories.

Goto Index

DNS Builder

DNS builder is used to build DNS server in less than 15 minutes. We use BIND for building DNS Server. Whitelist, Blacklist, Genius, RPZ and Categories are the Auto generated Zone files. Genius Zone file gets updated every 60 minutes via Pro-Active Cloud based Security Intelligence API. Whitelist and Blacklist zone files are manually controlled Zone files. DNS Server can be hosted in Public Cloud or Private Cloud.

Proxy Builder

Proxy Builder is used to build Proxy server in less than 15 minutes. We use SQUID for building Proxy Server. Proxy server features are Explicit Proxy, LDAP Authentication, Web-based reporting, SSL Inspection, Keyword Analysis, Domain Analysis, URL Analysis and File extension Analysis. Proxy Server is connected to Pro-Active Cloud based Security Intelligence API. Proxy Server can be hosted in Public Cloud or Private Cloud.

IDS Signature / Rules Builder:

IDS Signature builder gets its Updated rules/Packet Signatures from Open Source Emerging Threats, URLHAUS, FEODOTRACKER, Quadrantsec, Cisco, Talos Intelligence, Network Forensic,160Day rules, SSLBL and Aggressive rules. We also build Custom rules/signatures updated in IDS Signature builder.

Our Products:

DNS Firewall

Proxy Server

Browser Extensions/AddOns

Antivirus

Integrated IDS and L3 Catalyst Switch Automation

Secure Corporate Network Architecture

Secure VPN Teleworking Architecture

Goto Index

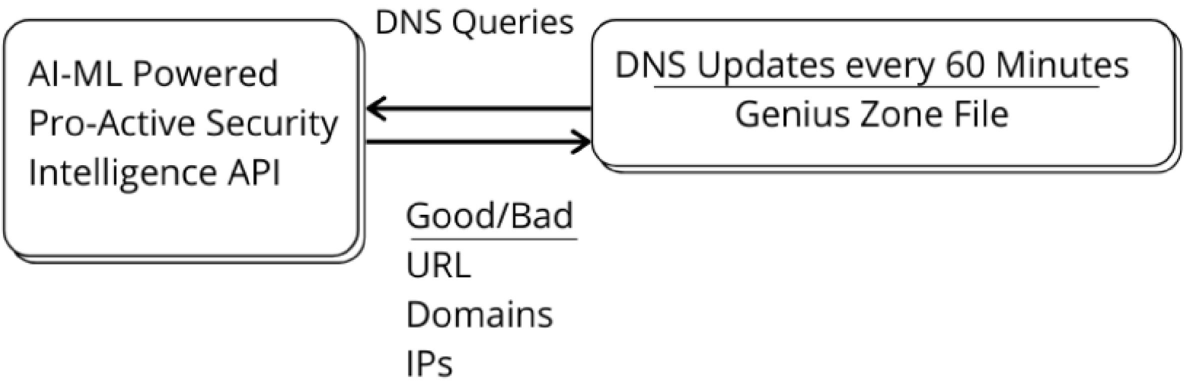
A DNS Firewall is a network security solution that prevents network users and systems from connecting to known malicious Internet locations. DNS Firewall works by employing DNS Response Policy Zones (RPZs) and actionable threat intelligence to prevent data exfiltration.

DNS Firewalls can also provide insights on threats, helps isolate infected devices for remediation, and stays current with the evolving threat landscape through an automated threat intelligence feed.

DNS Firewall is the leading DNS-based network security solution which contains and controls malware that uses DNS to communicate with C&Cs and botnets. DNS Firewall works by employing DNS Response Policy Zones (RPZs) and actionable threat intelligence.

DNS Firewall Powered by, Auto DNS Builder (Takes less than 15 mins) using Intelligent Threat Vector

- Manual Whitelist Zone File
- Manual Blacklist Zone File
- AI-ML Powered Genius/Category Zone File - Updates every 60 Mins
- Auto Open Source Intelligence Zone File - Updates every 60 Mins
- Auto Open Source Category Zone File - Updates every 60 Mins
- Connected to Pro-Active Cloud based Security Intelligence API



Goto Index

A **Proxy server** acts as a gateway between you and the internet. It's an intermediary server separating end users from the websites they browse. Proxy servers provide varying levels of functionality, security, and privacy depending on your use case, needs, or company policy.

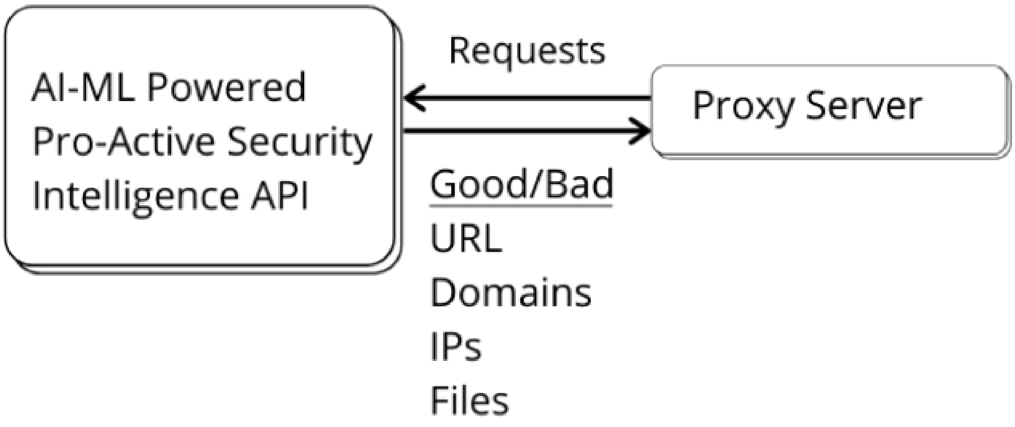
If you're using a proxy server, internet traffic flows through the proxy server on its way to the address you requested. The request then comes back through that same proxy server (there are exceptions to this rule), and then the proxy server forwards the data received from the website to you.

Proxy servers act as a firewall and web filter, provide shared network connections, and cache data to speed up common requests. A good proxy server keeps users and the internal network protected from the bad stuff that lives out in the wild internet. Lastly, proxy servers can provide a high level of privacy.

HTTPS-traffic is encrypted using the SSL (Secure Sockets Layer) protocol. SSL is designed to protect information being transmitted against eavesdropping. However, HTTPS traffic may present security threats, carrying malicious traffic or used as a cover up for illicit employee activities. With the help of SSL Bump, HTTPS proxy can decrypt and log into access.log requests transmitted over the HTTPS protocol. This in turn enables logging all user requests.

Proxy Server Powered by, Auto Proxy Builder (Takes less than 15 mins) using Intelligent Threat Vector

- Explicit Proxy
- LDAP Authentication
- Web-based reporting
- SSL Inspection
- Keyword Analysis
- Domain Analysis
- URL Analysis
- File extension Analysis



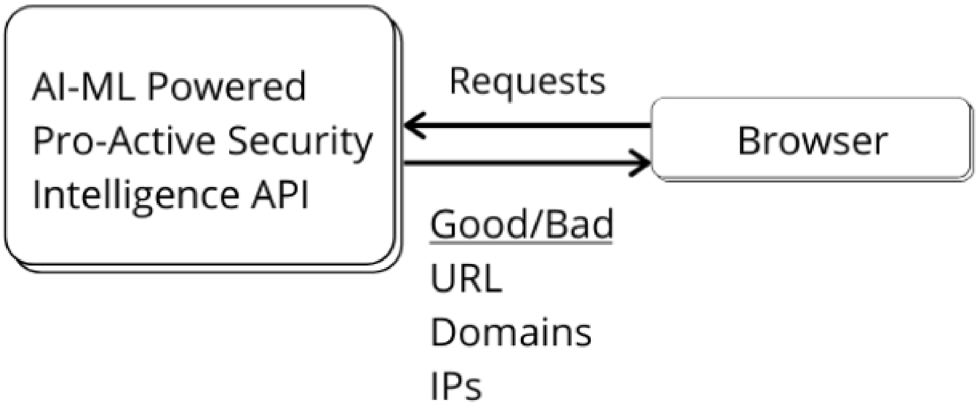
Goto Index

A **Safe Browser** is a web browser with extra security measures that help prevent unauthorized third-party activity while you're surfing the web. These browsers have a white list, or a list of authorized programs and activities, and they prevent functions that are not on that approved list from starting up.

While you may be familiar with anti-spyware and antivirus software, which react after a threat becomes apparent, safe browsers prevent certain actions from happening in the first place, making it a very proactive way to stay safer on the internet.

Browser Extensions Powered by, Pro-Active Cloud based Security Intelligence API,

- URL Prediction
- Domain Prediction
- IP Address Spam Analyzer
- Auto Redirection on Threat Detection

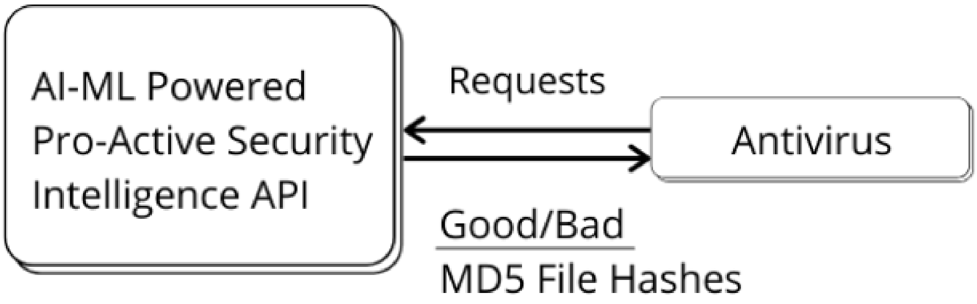


Goto Index

Online Antivirus is a kind of software used to prevent, scan, detect and delete viruses from a computer. Once installed, most antivirus software runs automatically in the background to provide real-time protection against virus attacks.

Antivirus Powered by, Pro-Active Cloud based Security Intelligence API,

- Full Scan
- Custom Scan
- Zero System Performance Impact
- Customizable
- Quick access to Logs



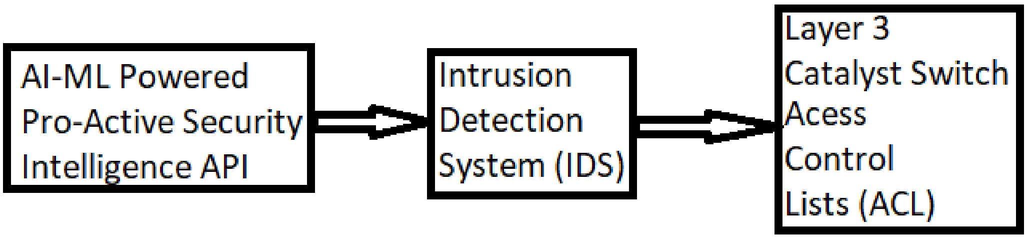
An **Intrusion Detection System (IDS)** is a network security technology originally built for detecting vulnerability exploits against a target application or computer. Intrusion Prevention Systems (IPS) extended IDS solutions by adding the ability to block threats in addition to detecting them and has become the dominant deployment option for IDS/IPS technologies. This article will elaborate on the configuration and functions that define the IDS deployment.

An IDS needs only to detect threats and as such is placed out-of-band on the network infrastructure, meaning that it is not in the true real-time communication path between the sender and receiver of information. Rather, IDS solutions will often take advantage of a TAP or SPAN port to analyse a copy of the inline traffic stream (and thus ensuring that IDS does not impact inline network performance).

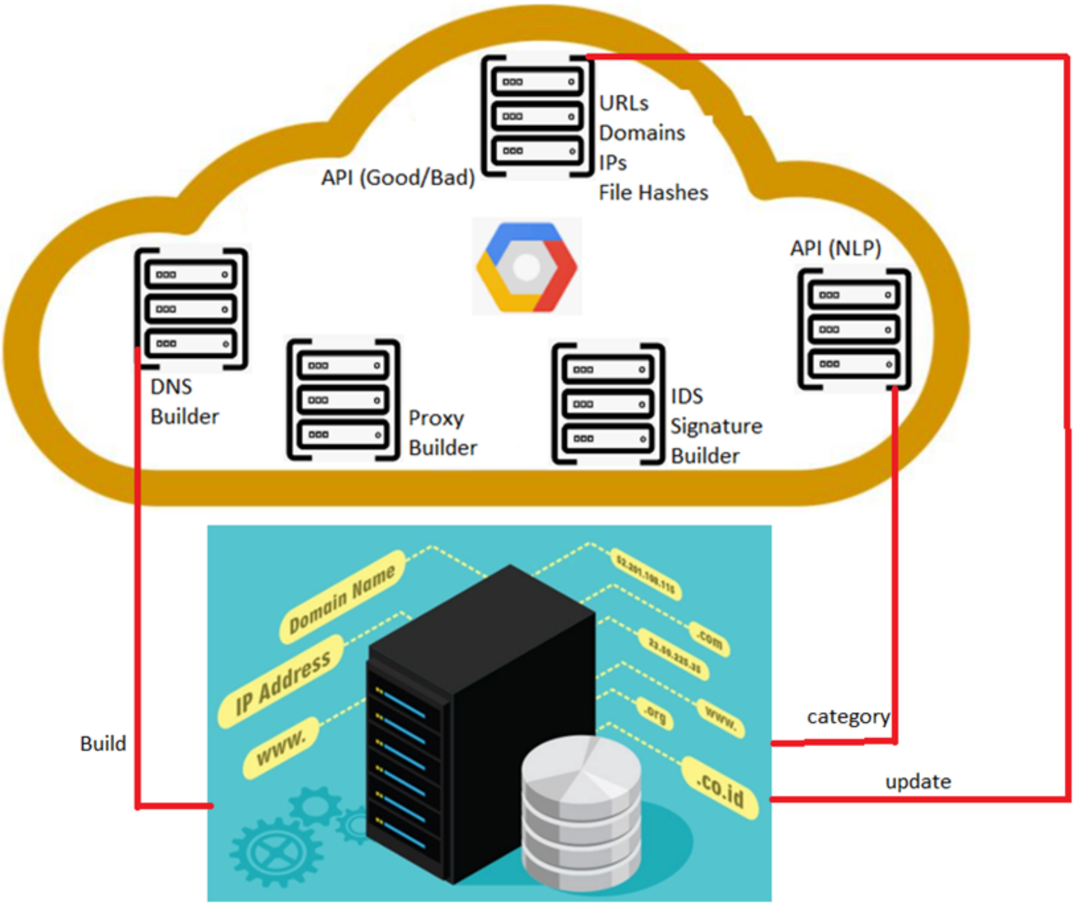
IDS was originally developed this way because at the time the depth of analysis required for intrusion detection could not be performed at a speed that could keep pace with components on the direct communications path of the network infrastructure.

As explained, the IDS is also a listen-only device. The IDS monitors traffic and report its results to an administrator, but cannot automatically take action to prevent a detected exploit from taking over the system. Attackers are capable of exploiting vulnerabilities very quickly once they enter the network, rendering the IDS an inadequate deployment for prevention device.

Intrusion Detection System (IDS) and Layer 3 Catalyst Switches are integrated together to behave like an Internet Firewall. For every 24 hours IDS Signatures/Rules are updated to IDS from Pro-Active Security Intelligence API.IDS will be actively listening to corporate LAN traffic and generates logs when there is packet signature match, providing the destination public IP address. IDS talks to Layer 3 catalyst switch to auto generate Access Control Lists (ACL) then and there. The Access Control Lists (ACL) will be flushed every 24 hours (midnight) in Layer 3 Catalyst Switch.

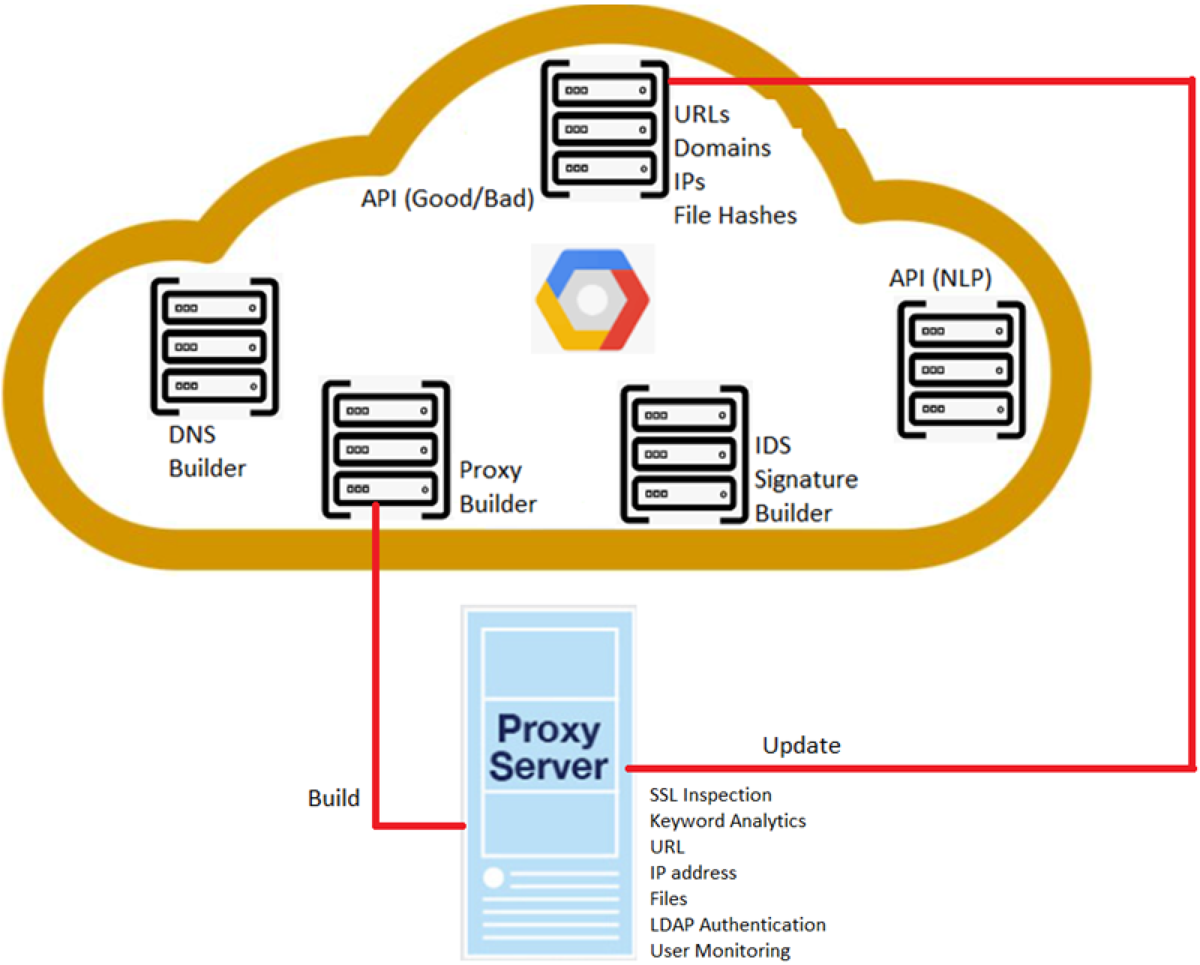

AI-ML Powered Pro-Active Security Intelligence API
Intrusion Detection System (IDS)
Layer 3 Catalyst Switch Acess Control Lists (ACL)

DNS Builder and DNS Server Update Flow Diagram:



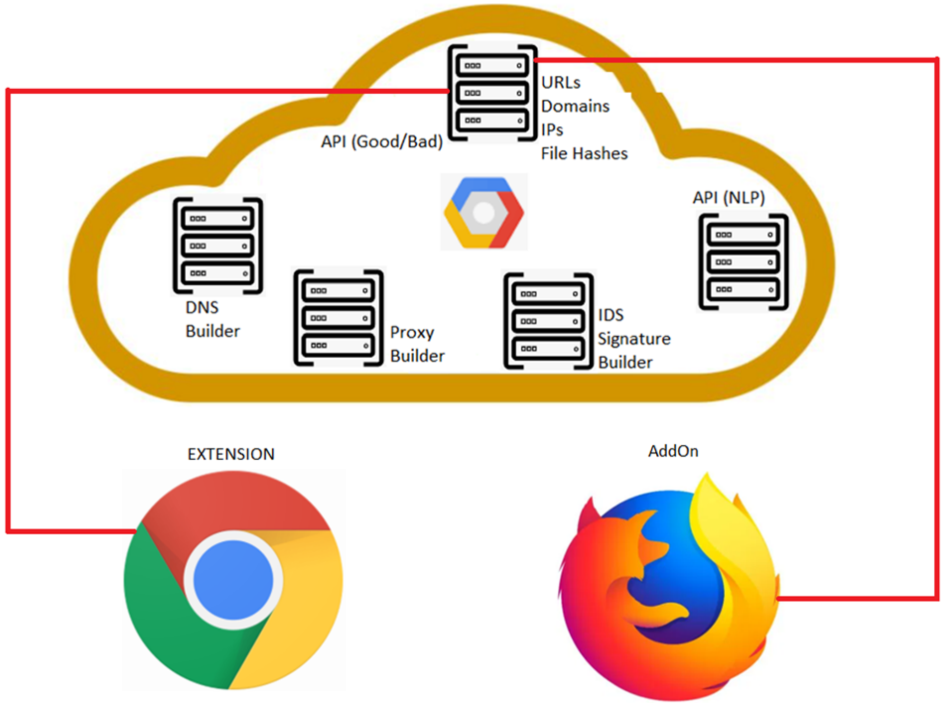
Goto Index

Proxy Server Builder and Proxy Server Update Flow Diagram:

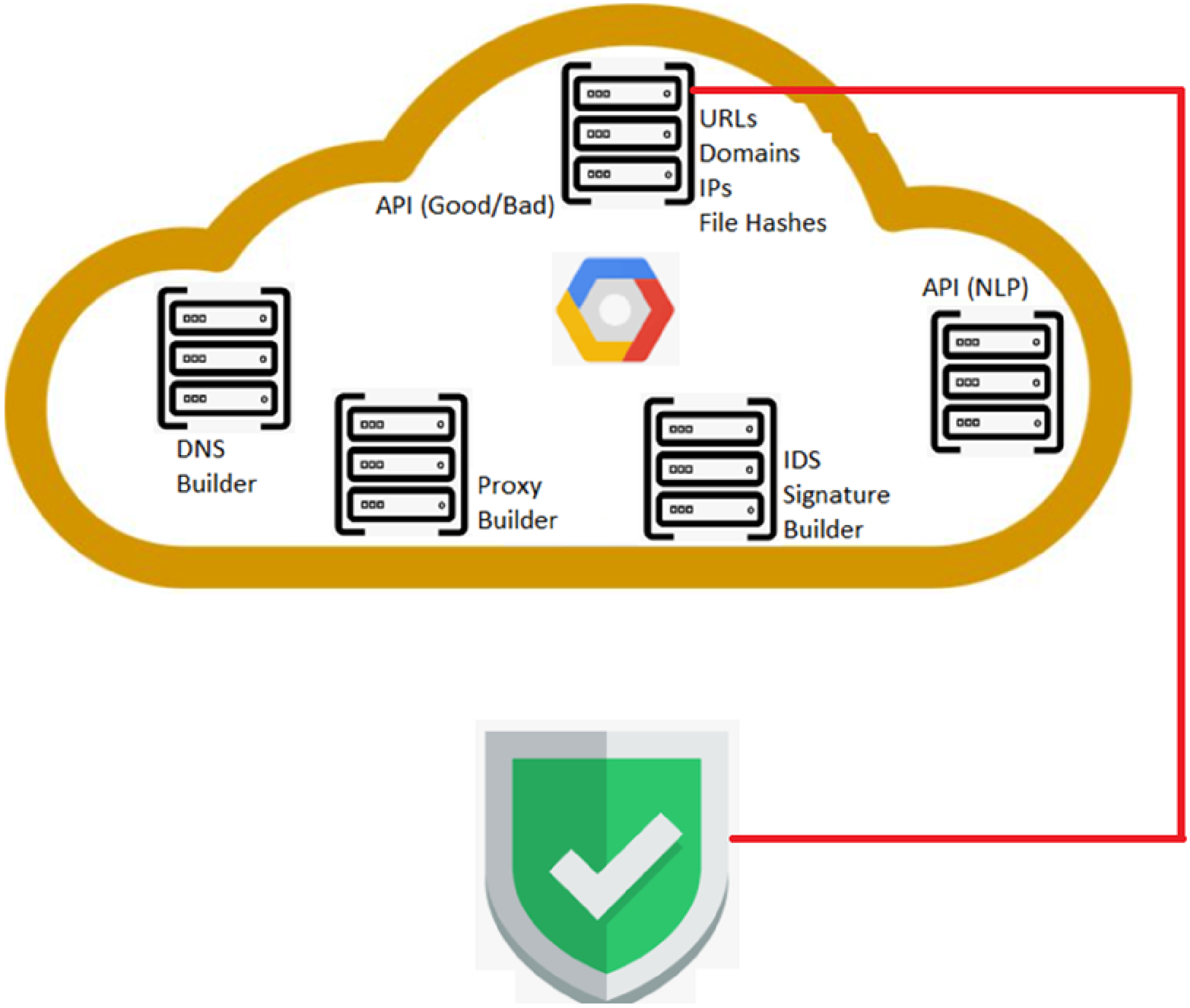


Goto Index

Browser Security Update Flow Diagram:

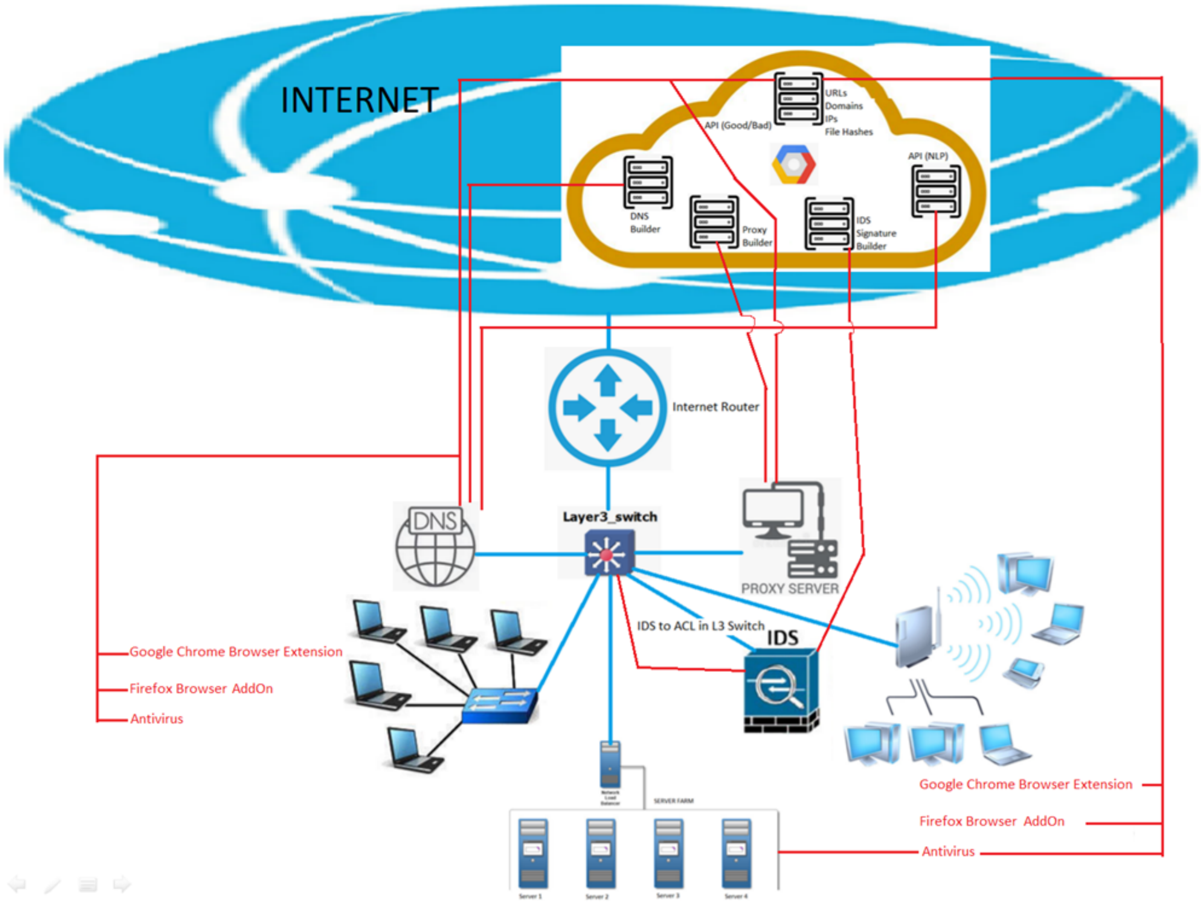


Antivirus Update Flow Diagram:



Goto Index

Secure Corporate Network Architecture:



DNS Server

Inspects corporate LAN queries. It is connected to three APIs called DNS Builder, API(Good/Bad) for Domain/IP Address validation and API(NLP - Information Categorization).

Proxy Server

Inspects corporate LAN Users and URLs requests. It is connected to API(Good/Bad) for URL validation.

Chrome/Firefox Extension/AddOn

It is connected to API(Good/Bad) for URL validation.

Antivirus

It is connected to API(Good/Bad) for MD5 file hash validation.

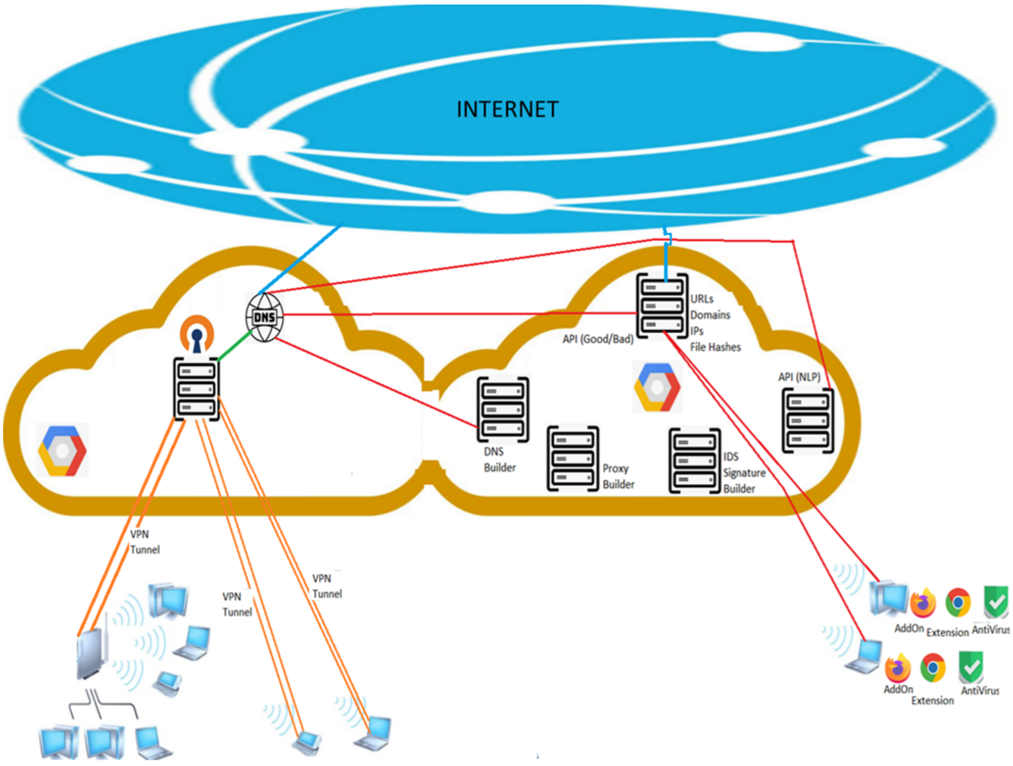
Goto Index

IDS integrated to Catalyst Layer 3 Switch :

IDS Signature builder gets its Updated rules/Packet Signatures from Open Source Emerging Threats, URLHAUS, FEODOTRACKER, Quadrantsec, Cisco, Talos Intelligence, Network Forensic,160Day rules, SSLBL and Aggressive rules. We also build Custom rules/signatures updated in IDS Signature builder.

Intrusion Detection System (IDS) and Layer 3 Catalyst Switches are integrated together to behave like an Internet Firewall. For every 24 hours IDS Signatures/Rules are updated to IDS from Pro-Active Security Intelligence API.IDS will be actively listening to corporate LAN traffic and generates logs when there is packet signature match, providing the destination public IP address. IDS talks to Layer 3 catalyst switch to auto generate Access Control Lists (ACL) then and there. The Access Control Lists (ACL) will be flushed every 24 hours (midnight) in Layer 3 Catalyst Switch.

Secure VPN Teleworking Architecture:



In Secure VPN Teleworking Architecture, the VPN access server in the public cloud is enforced to use custom DNS Server IP address. When VPN client users initiate VPN connection to browse Internet with privacy, the users will be forced to use the enforced custom DNS IP, irrespective of the DNS IP address provided by any ISPs of the users. Thereby providing both Privacy and Security while accessing the Internet.