eNlight Web VPN Service

ESDS Software Solution Pvt. Ltd.

eNlight Web VPN Service

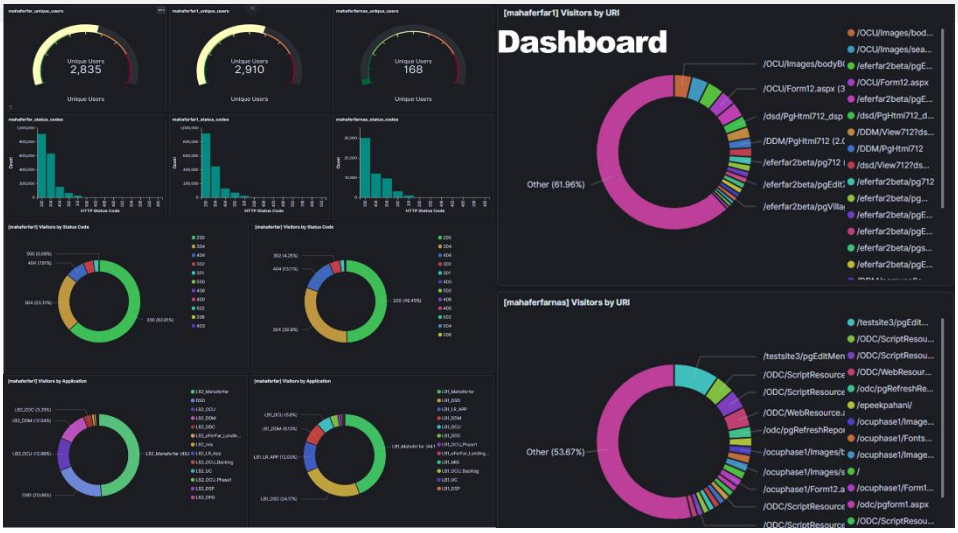
For secure access

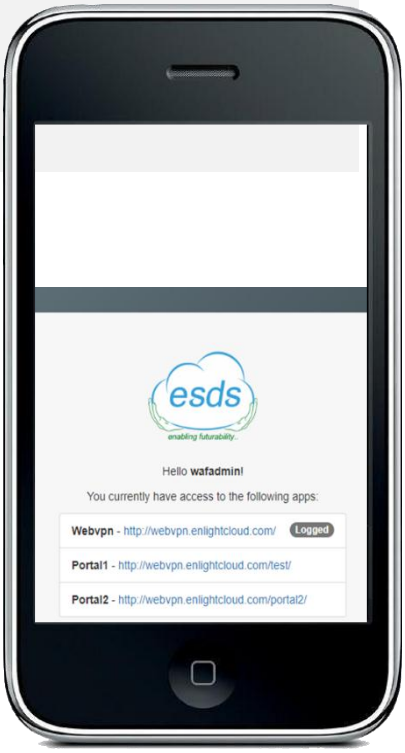
eNlight WebVPN is specially engineered intelligent cloud hosted unique clientless VPN solution with built-in WAF for Layer7 security, high performance incoming TCP load-balancer (self-LB) and proxy balancer (backend server LB) to have powerful multi-layered load-balancing that allows you to access privately hosted applications, more securely & supports SSH, Websocket, RDP, FTP protocols. WebVPN is highly available and scalable due to its unique multi-layered LB.

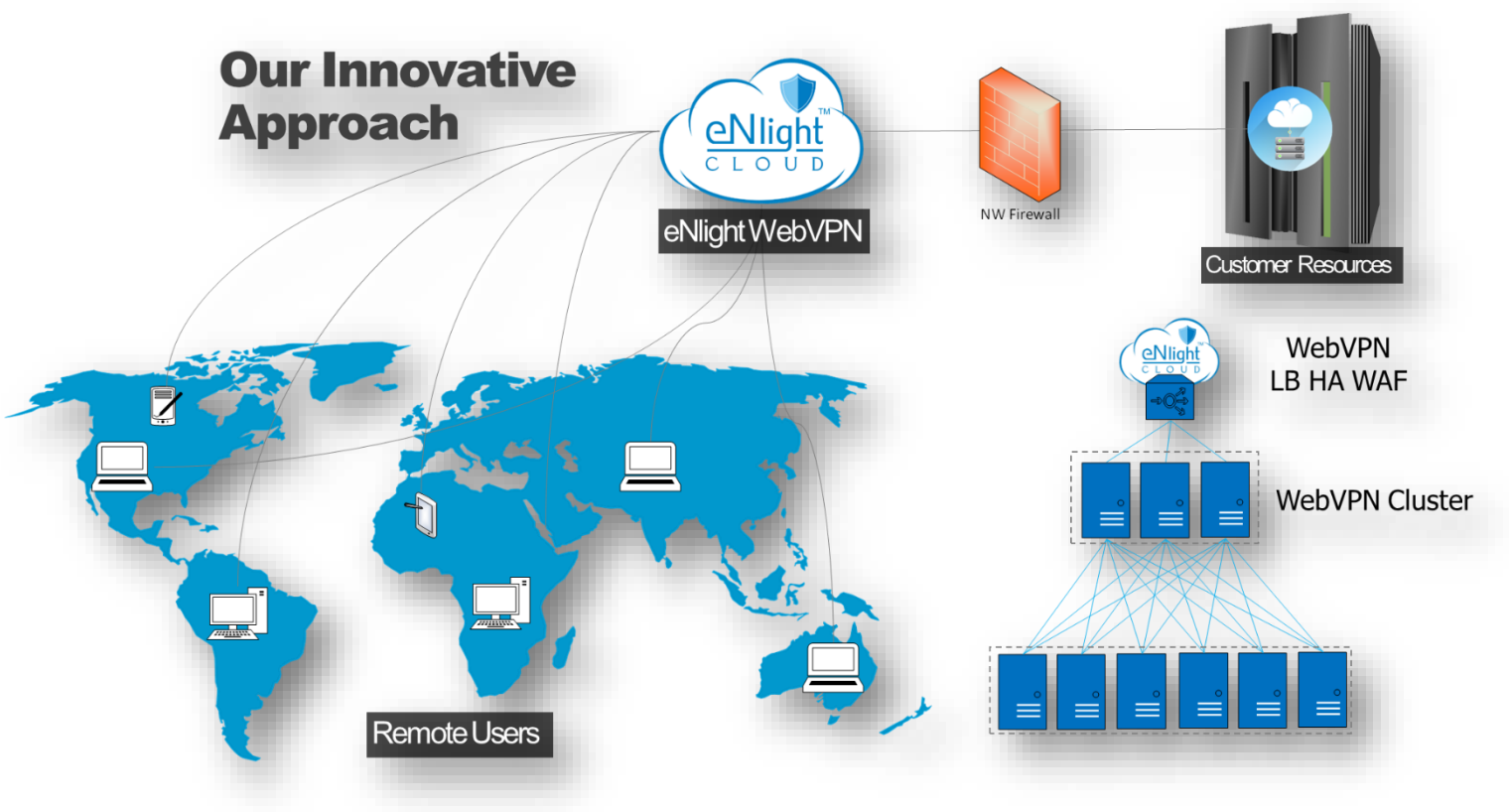
- Supports multiple desktop and mobile platforms including Windows, MAC, and Linux, mobile OS (Android and iOS) environments
- Easily integrate with existing authentication services: LDAP, Active Directory(AD), Kerberos, SQL, Radius for user authentication and authorization
- Built-in support for 2 factor authentication methods –
- Multifactor authentication with SMS and Email OTP
- Time based OTP with Google and Microsoft Authenticator
- Easy web-based management, role-based administration, detailed audit and logs for incident isolation and troubleshooting
- Built-in support for WAF customizable rulesets and policies
- Supports for HTML5 applications, Websocket, RDP, FTP protocols, CGI applications
- WAF protects from OWASP Top 10 Vulnerabilities

ESDS clients can now utilize exclusive eNlight web VPN services

- ***Access your web- applications from anywhere***
- ***Completely clientless VPN solution***
- ***Authorize & Protect***







Security
Enable TLS, control user reputation, set up access control and block OWASP Top 10 attacks (XSS, SQL Injection, Malware) before they reach your web applications

High Availability
Need to increase the traffic handling capacity? Add nodes to the cluster: WebVPN runs natively as horizontally scalable active/active cluster

Load Distribution
WebVPN distributes incoming traffic to all nodes in the cluster. WebVPN can then dispatch the traffic to a farm of Web servers.

Content Rewriting
WebVPN works in reverse-proxy. You can rewrite links, headers, content, compress pages

Anomaly Detection
WebVPN integrates anomaly detection algorithms allowing the administrator to identify risky behaviors and create effective filtering policies. No need to invest in a SIEM to benefit log analysis, alerting or anomaly detection in real time.

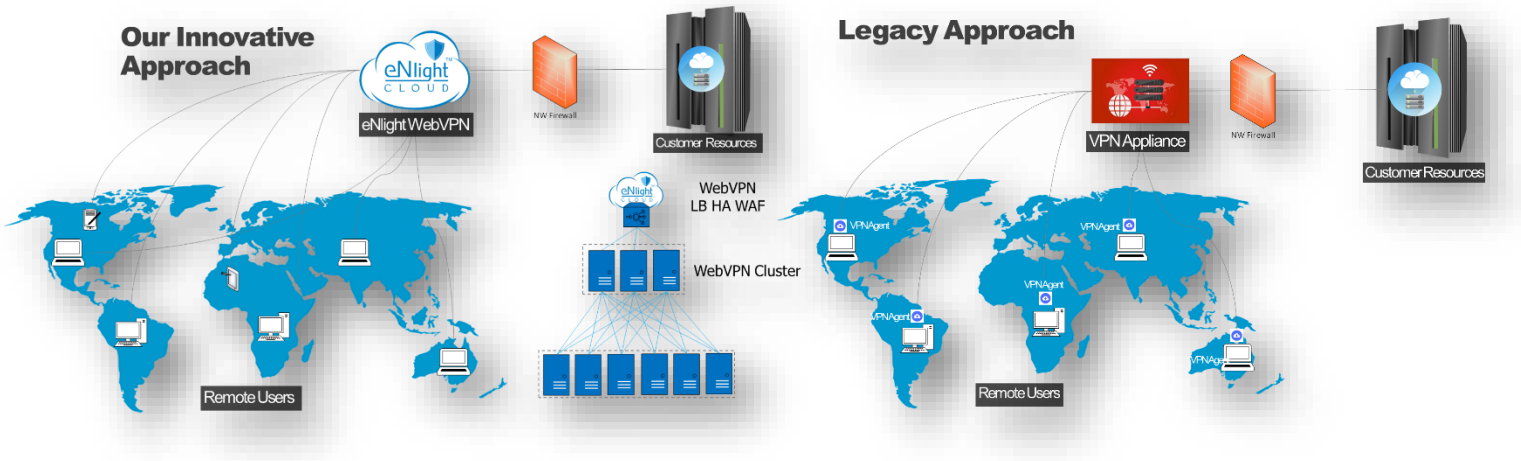
eNlight WebVPN Vs. Legacy VPN

eNlight WebVPN

- Clientless
- More secure - Gives access to only Applications
- Cost effective than legacy VPN
- Granular access control
- Don't need to reconnect when internet network changes
- Ease to deploy and use
- Scalable and HA
- Provides WAF and OWASP Top 10 vulnerability protection

Legacy VPN

- Client/Agent Based
- Less Secure - Gives access to whole Network
- Costly than webvpn
- Fixed access control
- Need to reconnect when internet network changes
- Complex to deploy and use
- Less scalable and HA
- WAF and other security features not available



eNlight WebVPN Technical Specs

- **Web Load Balancer**
  WebVPN can spread the load over multiple web servers and maintain application sessions.

- **Load-balancing IPv4/IPv6 network**
  Inbound traffic is distributed to all nodes in the cluster IPv4/IPv6 virtual addresses
  If one node fails, the others take over
  IPv4/IPv6 network firewall. Malicious IPs are blocked before they reach applications.

- **Source IP Reputation Analysis**
  WebVPN geo-localizes source IPs and analyzes their reputation It is possible to make filtering policies on these criteria. The blocking is done before processing the HTTP request.

- **Learning Mode**
  WebVPN records all suspicious requests without blocking the user. Administrator manages false positives without hindering user activity. When there is no more blocking identified, the learning mode is disabled and WebVPN goes into blocking mode.

- **Machine Learning**
  In addition to rule-based filtering and reputation of the sources, WebVPN proposes an approach based on mathematical algorithms:

1. Learning and modeling of typical traffic
2. Detection of "abnormal" requests

- **Log Analyzer**
  The logs are searchable from the administration interface. Quick and intuitive interface, possibility to save your search filters. Logs available: Firewall, WAF, access to applications, internal logs (API, diagnostic system etc.).

- **Supports multiple websites security**
  Supposing an organization has more than one website and wants to handle all the websites by WebVPN, that's possible with a single dashboard multiple websites can be handled.

- **Virtual Patching**
  Upload a vulnerability scanner report, WebVPN generates the rules to correct the identified vulnerabilities.

- **Scoring Policy**
  WebVPN makes the decision to block when the risk score exceeds the threshold tolerated. The administrator decides score threshold policy.

- **OWASP Top 10 Protection**
  Qualified and ready-to-use rules are integrated by default. Protection against OWASP Top 10 vulnerabilities. Automatic import, versioning rule sets, graphical interface to edit the rules, assistant for writing rules.