



Small and Medium Enterprise (SME) Sector

Security Router/UTM Product Line



OBJECTIVES

To set-up a secure network for a small and medium enterprise and to facilitate connectivity to the branch offices, and to the professionals working remotely.

CHALLENGES

Due to high demand of the company's products, the company decided to expand its business, and hence opened multiple branch offices to capture the desired market. The major challenge faced by the enterprise was to have secure communication between its offices. Each office is equipped with a router which connects to the router present in the other office building. The company needs to connect the multiple sites efficiently in a cost-effective way.

To transfer the information from one branch office to the other, internet is being used. The information transferred between the offices should not be hacked and should be as secure as a wired network. But there have always been known issues with the internet security, and hence this is a matter of major concern for the enterprise.

While understanding the company's work environment, it was also found that they have a team that works remotely and are unable to access office server when not in office. The company was looking forward to a solution that could provide them access to the office server continuously.

Apart from connectivity between the branch offices, the enterprise has to be careful if any confidential information is being shared by any employee with an unknown person. A provision to scan and block such confidential information from being shared, is required by the IT department of the company.

Providing internet access to a guest is also one of the requirements these days. For this, a web authentication is required.

SOLUTIONS

D-Link's initial steps included identifying the office locations and their present networking facility. It was also important to know that how many people are using the network at a time. To provide secure communication between the offices sited at multiple locations, and a fast wireless network, D-Link chose its Security Router based on the latest technology with the software package from TeamF1 Networks. D-Link Security Router supports 2.4 GHz and 5 GHz dual-band wireless with VPN speed up to 250 Mbps and Firewall speed up to 950 Mbps.

D-Link Security router can work as a Gateway, VPN, and UTM. The Gateway router supports Load balancing feature which distributes network traffic among multiple Internet Providers. It improves the network performance and network availability. The QoS (Quality of Service), which includes Traffic Management and Traffic shaping, is used to utilize the internet bandwidth efficiently and to prioritize the network traffic which reduces the impact of heavy internet usage users from effecting other users.

To connect to the multiple offices, VPNC certified D-Link Router supports Gateway to Gateway VPN (Virtual Private Network) which allows these offices to transport data in an encrypted form. It uses IP Security (IPsec) Protocol, Point-to-Point Tunneling Protocol (PPTP), GRE, or Layer 2



Tunneling Protocol (L2TP) to facilitate branch office connectivity through encrypted virtual links. The D-Link Security Router product line supports up to 100 simultaneous IPsec VPN tunnels. IPsec tunnel mode is preferred as it encrypts the original data packets and transfers it to the other end of the tunnel.

Remote access VPN, i.e. Client to Gateway VPN, is a solution to provide access to the company's server to the employees who are working remotely or travelling frequently. The individual users can easily get connected to the private network, provided every user has a VPN client.

The DSR-series supports Unified Threat Management and comes with Intrusion Detection and Prevention System (IDS/IPS) which reviews every packet for malicious attacks. The device is capable enough in blocking Denial-of-Service (DoS) attacks, can configure thresholds for ICMP packet flooding, SYN traffic flooding, and Echo storm to temporarily suspect traffic from the offending source. These features help users to manage WAN security threats easily.

D-Link, being ICSA Certified, increases the security of WAN port by allowing the user to define firewall rules, both IPv4 and IPv6 Firewall rules, for inbound and outbound traffic. The gateway also offers standard web filtering options to allow the admin to easily create internet access policies between the secure LAN and insecure WAN. Instead of creating policies based on the type of traffic (as is the case when using firewall rules), web based content can be used to determine if traffic is allowed or dropped.

D-Link DSR supports Captive Portal which allows employees and guest users of the enterprise to get easily authenticated with custom login page. The captive portal is provided to the specific SSIDs for a certain period of time. D-Link Security Router has a USB interface for printer access, file sharing and 3G/4G modem support. A 3G modem dongle can be plugged in and used as a secondary WAN. Load balancing, auto-failover, or primary WAN access can be configured through the 3G/4G.

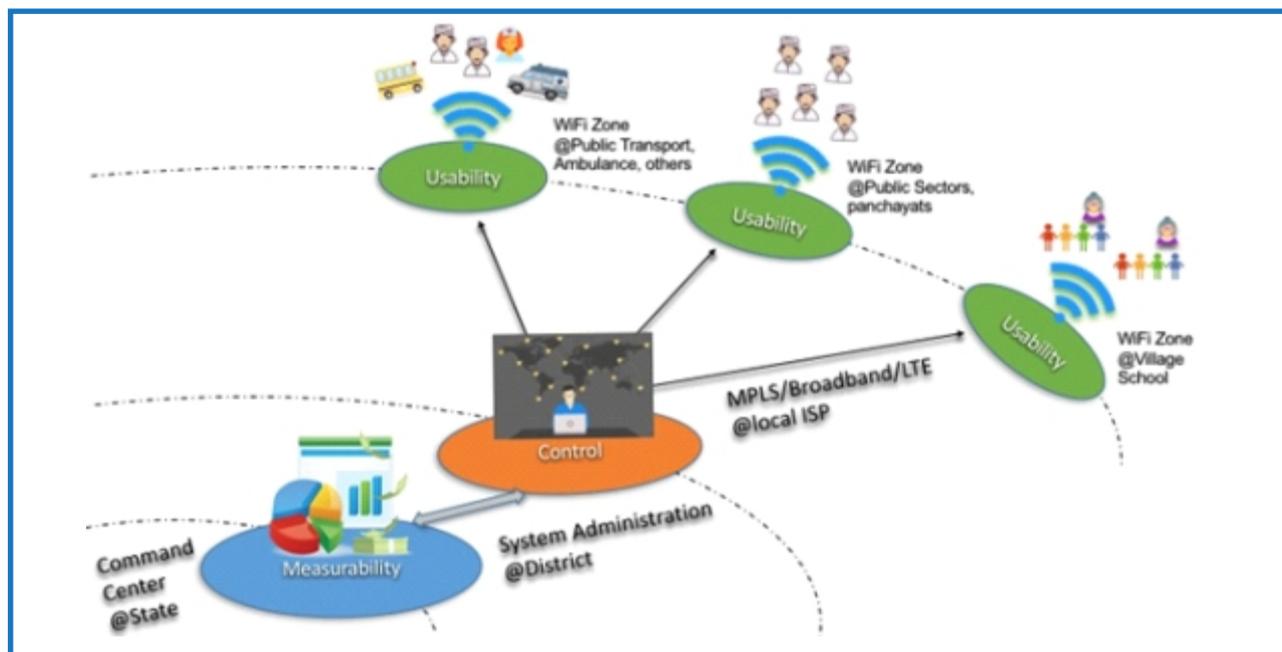
SOFTWARE PACKAGE BY TEAMF1

TeamF1 Networks' products enable secure networking of telecom or Datacom, and industrial equipment, and provide the infrastructure components needed for switching and wireless products in various market segments. TeamF1 Networks leverages pre-existing software blocks that have proven their merit in thousands of deployments, minimizing risk for OEMs and Service Providers (SPs) at flexible licensing terms. TeamF1 provides the best solution for SMB security gateways that require UTM/VPN/firewall/router features with comprehensive management capabilities.

RESULTS

The installation of D-Link Security Routers and its complete and robust VPN features like IPsec, L2TP, PPTP, GRE, and OpenVPN have resulted in a secure connection between the offices located at multiple places. The gateway-to-gateway VPN has enabled the enterprise to connect and transport data using encryption and other security protocols. The employees who are working remotely or who are travelling frequently can now be connected to their corporate network and can work from anywhere at any time using VPN client.

The Firewall and UTM capabilities of D-Link's DSR series have protected the network from external malicious attacks using IDS/IPS, Attach Checks, Web Content Filtering, and Blocking URLs and keywords. It provides a reliable, and secure wireless network suitable for small and medium enterprises located at multiple places.



Illustrating key elements in play with critical use-cases

TeamF1 Networks

TeamF1 Networks specializes in developing high-performance networking and security software products, which help in future-proofing the digital network connectivity and security roadmap for embedded devices. TeamF1 Networks' network security solutions empower wired and wireless devices world-wide for small and medium businesses and residential networks. This includes applications ranging from business security gateways, UTM firewalls and network storage devices to home gateways and service provider routers.

The access points scattered at multiple geographical locations to provide seamless connectivity can also be remotely controlled using the latest and proven technology "Cloud Computing." TeamF1 Networks provides Cloud Solution which has the ability to virtually manage, monitor, and control the widely spread APs and push configuration to all the APs at one go without adding any delay. It also provides continuous auto-updates to the client in case latest updates are available. This provides massive scalability, providing virtually unlimited resources to the client. The software or additional devices for network expansion can be easily deployed from any location through remote management.



TeamF1 Networks (P) Ltd.

(Subsidiary of D-Link (India) Ltd.,)

📍 5th Floor, Block-1, My Home Hub, Hitech City,
Madhapur, Hyderabad - 500081. Telangana, India.

☎ Phone (India) : +91 (0) 40662 87500

✉ E-mail : pr@teamf1networks.com

