Level 3 COMMUNICATIONS

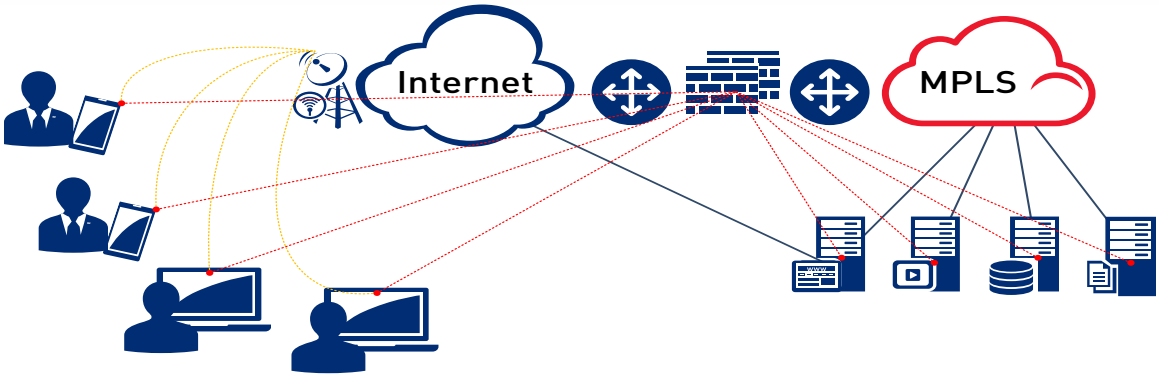
Connecting and Protecting the Networked World℠

LEVEL 3℠ SECURE ACCESS

MOBILITY

Help enhance the productivity of your mobile workforce with this scalable and secure solution, providing remote VPN access (IPsec or SSL VPN) to your company network. Giving you the tools to securely manage employee remote connectivity while maintaining centralized user access policies.

Today's businesses require comprehensive mobile workforce management. Whether you are a large multinational corporation or a regionally based business, chances are you need to provide both resources and support to mobile employees. As your organization expands and the "Bring Your Own Device" (BYOD) trend grows, so does the complexity of ensuring secure connectivity to your corporate resources. Level 3℠ Secure Access Mobility Service connects remote users or teleworkers to your network via IPsec or SSL-based Internet connections and a standard web browser. Whether they connect with a laptop, tablet or smartphone, you have the ability to securely manage employee remote connectivity in this diverse and evolving environment.



No matter the dynamics of your business, if you have a mobile workforce with the need to travel, connectivity and security can be two of your biggest concerns. As the BYOD trends permeate your business, the task of managing users and different devices can become overwhelming for even the seasoned IT professional. Let Level 3 help with our Level 3 Secure Access Mobility solution which can help enable your workforce to connect to your corporate network from anywhere around the world, on almost any device while providing centralized management tools for authentication, user role mapping, resource and sign-in policies. This way your staff can keep an eye on devices, users and permissions to ensure only authorized personnel have access. Our solution can foster productivity within your staff, no matter the setting, providing access to business critical applications anywhere, anytime, while helping to ensure your data is moving securely and your infrastructure/systems are being accessed by the appropriate parties.

Level 3 COMMUNICATIONS

Connecting and Protecting the Networked World℠

Business Solutions

Scalable – Extensive global footprint available as a network-based solution for mobile connectivity with gateways on four continents and the flexibility and capacity to grow with your business.

Low cost – Help reduce your capital outlay and control headcount/IT staff with a predictable monthly cost and no upfront capital expenditure or continued investment in hardware or software to add more users.

Maintain business continuity – Help to ensure employees traveling or out in the field have secure access to necessary resources.

Simplify IT Management – Help to securely manage employee remote connectivity in a BYOD environment with centralized management for authentication, user role mapping, resource policies and sign-in policies

Security – IPsec and SSL provide end-to-end encryption and tunneling to help meet the challenges of transmitting unencrypted text and help to ensure that your company's private data remains secure.

By 2015, it is expected that the world's mobile worker population will reach 1.3 billion or 37.2% of the total global workforce.

(IDC WORLDWIDE MOBILE WORKER POPULATION 2011-2015 FORECAST DOC#232073)

Technical Features/Capabilities

Equipment – Juniper (SA) 6500

- Supporting 50-1,500 users
- IPsec (VPN Tunneling) or SSL VPN (Web Access) connectivity options

IPsec

Support for full VPN capability on supported clients using IPsec and/or SSL as the transport mechanism

Split tunneling is standard

Standard transport mechanism is ESP, AES/128 SHA1 standard encryption

Software must be installed on client device (Network Connect or Junos Pulse Client)

Host Checker is supported with web browsers and the Pulse/Network Client but is not standard, requiring a security consulting engagement

SSL VPN

Multiple access options

- Web URL access
- Terminal services
- Telnet/SSH
- File access

Traffic is permitted to RFC 1918 address space

One landing page per customer

Does not require specialized software to be placed on remote devices

Host checker is supported with web browsers and the Pulse/Network Client but is not standard, requiring a security consulting engagement

SSL VPN Access Options:

Web URL access

Microsoft® Outlook® Web Access, SharePoint® and Citrix® Web Interface

The standard number supported with this service is ten.

For general URL access, only Web ACL and Single Sign-on (SSO) policies will be supported

Terminal services

Limited to Windows®, Linux® and MAC® clients.

The standard number supported with this service is two

Telnet/SSH

Support is limited to Windows, MAC and Linux clients

The standard number of connections supported with this service is two

Level 3 COMMUNICATIONS

Connecting and Protecting the Networked World℠

File access

SSL VPN access to Windows and Unix File Shares leverages Single Sign-on for statically added resources

The standard number of connections supported with this service is two

Globally dispersed VPN gateways:

- NA: New York, Houston, Sacramento
- EMEA: London, Amsterdam
- LATAM: São Paulo
- APAC: Hong Kong

Multiple devices supported with an Internet connection and web browser

Mobile and local device support; covering Windows®, MAC, Linux®, Android™ and Apple® iOS platforms.

Internet Explorer®, Firefox®, Safari®, Chrome™

Access management:

Supports utilization of various authentication systems to include Windows Active Directory (AD), LDAP and RADIUS

Customers using AD will also have single sign-on

The default is to support one authentication realm and up to two authentication servers.

Services supported with either Level 3 or customer managed RADIUS service.

User Role(s): The customer has the option to define up to three roles as a part of the standard configuration.

User Role Mapping: Support of role mapping via username and group membership can be done when active directory and/or LDAP authentication/directory servers are configured within the specific realm.

Resource policy(s): The supported resource policies are broken down based on service type categories such as Web Access, File Access, Telnet/SSH, Terminal Services and VPN tunneling.

Sign-in policies: One sign-in page is standard with the service.

24 x 7 proactive support: Our expertise and monitoring systems are designed to detect the health of your solution. We provide device and service proactive monitoring with sophisticated threat identification and protection tools.

Real time security reporting: audit reporting with a client connection summary providing data about connections over time, connections by user, failed connections by user, connections by realm and connections by role and last 20 Juniper Events

Why choose Level 3 for managed security?

Global network & threat data - Our global collection of IP, CDN, DNS and MPLS network assets provides us an exceptional view into the threat landscape and tremendous amounts of attack data, enabling us to help identify threats, correlate data and identify/mitigate threats more quickly.

Security Operations Center (SOC) – Enjoy the simplicity of a single point of contact with the Level 3 Security Operations Center (SOC) staffed 24 x7 with analysts and engineers who stand ready to proactively and efficiently respond to your security issues, including physical and logical alarms, attacks, suspicious or abnormal network activity, and assist with your security inquiries.

Simplifying Vendor Complexity – The suite of Level 3 Security Services was created to integrate seamlessly with our entire global portfolio of network services, so you can buy and manage everything you need in one place.

ABOUT LEVEL 3

We build, operate and take end-to-end responsibility for network solutions that connect you to the world. We put customers first and take ownership of reliability and security across our broad portfolio.

1.877.2LEVEL3
INFO@LEVEL3.COM
LEVEL3.COM

DATA NETWORKS | SECURITY | CONTENT DISTRIBUTION | DATA CENTERS | APPLICATION PERFORMANCE | VOICE | UCC