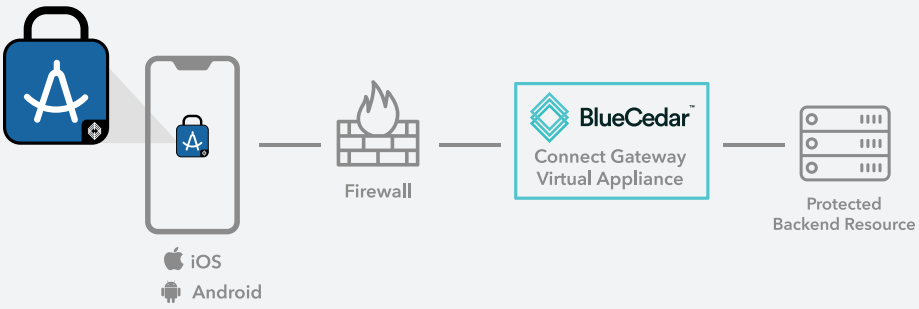
BlueCedar™

DATA SHEET

Blue Cedar Connect Gateway

The Blue Cedar Connect Gateway is an IKEv2 VPN gateway and a key component of Blue Cedar's secure connectivity offering, which enables organizations to rapidly make the digital-first transformation. The Blue Cedar Connect Gateway allows apps integrated with the Blue Cedar Accelerator for Secure Edge Connect to securely access network protected resources such as backend services and application data. With Blue Cedar's secure connectivity offering, enterprise users can seamlessly connect to remote resources from any device, even one not controlled by MDM.



This diagram shows the deployment of the Blue Cedar Connect Gateway as part of Blue Cedar's secure connectivity offering. On the left side of the diagram is a mobile app into which a VPN client has been integrated without coding through the use of the Blue Cedar Accelerator for Secure Edge Connect.

Benefits

Safer and Better Online Experience
Support for the Internet Key Exchange version 2 (IKEv2) VPN encryption protocol means that enterprises can benefit from all the associated improvements. IKEv2 provides better security because of support for IPSec's latest encryption algorithms and other encryption ciphers such as NSA Suite B cryptography. IKEv2 provides better connectivity with fast online speeds that do not degrade or get interrupted when networks change, and dropped VPN connections automatically re-establish. Also, IKEv2 provides lower bandwidth usage than IKEv1, resistance to DDoS attacks, and perfect forward secrecy (PFS).

FEATURES

- Support for IKEv2
- Static, DHCP and NAT address pool
- Delivered as a virtual appliance
- Deployable in the cloud or on-premises
- Cloud-configurable network interfaces
- In-place upgrades
- Validated on Microsoft Azure, AWS and VMware ESXi
- Authentication Mechanisms: LDAP, SLDAP, Local User Accounts, Microsoft AD, RADIUS and OAuth
- User Authentication: PSK, Client Certificates, 2FA and OAuth
- Inbound Port Protocols
  - Communication: UDP 4500, UDP 500
  - Authentication: TLS 443

SPECS

- Tested virtual machine specs
  - 2 CPU cores
  - 8 GB of RAM
  - ~60 GB storage
- Operating System: CentOS 7.6 or RedHat 7.6
- Networking interfaces: 2
- Concurrent connections: 2500 per virtual appliance

Reduce Costs
Each Blue Cedar Connect Gateway can support up to 2500 concurrent connections, which translates into a lower deployment footprint as well as lower maintenance costs. A new configuration option allows routing of all external connections through an internal NAT (network address translation) layer to appear on the internal network as a single address. The advantages of this feature are that each in-app VPN doesn't require its own internal IP address, and an organization's networking team does not have to spend time on allocating and managing a unique pool of addresses for all connecting mobile clients and apps.

Flexible Deployment Options
The Blue Cedar Connect Gateway is available as a virtual appliance that can be deployed on-premises or in the cloud. Use of a standard Linux distribution, a mode where networking interfaces can be configured by the cloud on which the virtual appliance is installed and support for in-place upgrades enable easy deployment in cloud environments. For on-premises deployments, users can configure the IP addresses and associated network information for each network port. The Blue Cedar Connect Gateway has been tested on the Microsoft Azure and Amazon Web Services (AWS) cloud environments, and the VMWare ESXi hypervisor. Two variants of the virtual appliances are available: one with CentOS 7.6 as the base OS and one with RedHat 7.6.

Enterprise Authentication Methods
The Blue Cedar Connect Gateway provides rapid authentication, which occurs over HTTPS. Support for a wide range of authentication mechanisms makes it easy to deploy in enterprise networks. Lightweight Directory Access Protocol (LDAP), Secure Lightweight Directory Access Protocol (SLDAP), Local User Accounts, Microsoft Active Directory (AD), Remote Authentication Dial-In User Service (RADIUS) and Open Authorization (OAuth) are the supported authentication mechanisms. Once the user is authenticated, the user can establish a connection with a combination of pre-shared keys (PSK), client certificates, OAuth and two factor authentication (2FA). Two factor authentication relies on a certificate and username/password.

Secure BYOD Access
No-code integration of in-app VPN ensures that apps executing on any device, even one not under MDM (Mobile Device Management) controls, can connect to remote enterprise resources through the Blue Cedar Connect Gateway without requiring end user configuration of the VPN client. By obviating the need for MDM controls on personal devices (the BYOD or Bring Your Own Device use case), enterprises can boost productivity by making backend services and application data usable by a broader swath of mobile users—all without compromising on security or impacting users' privacy.

Improve Usability
Integrated apps are automatically configured to create transient app-level secure microtunnels to internal resources through the Blue Cedar Connect Gateway. App usability improves as users can seamlessly connect and gain access to protected backend resources.

Lower Development Costs
The Blue Cedar mobile app integration platform uses the Blue Cedar Accelerator for Secure Edge Connect to embed Blue Cedar's in-app VPN clients into ISV and custom mobile apps without coding, enabling enterprises to save on mobile development costs.

325 Pacific Avenue, San Francisco, CA 94111
info@bluecedar.com / bluecedar.com

08212019