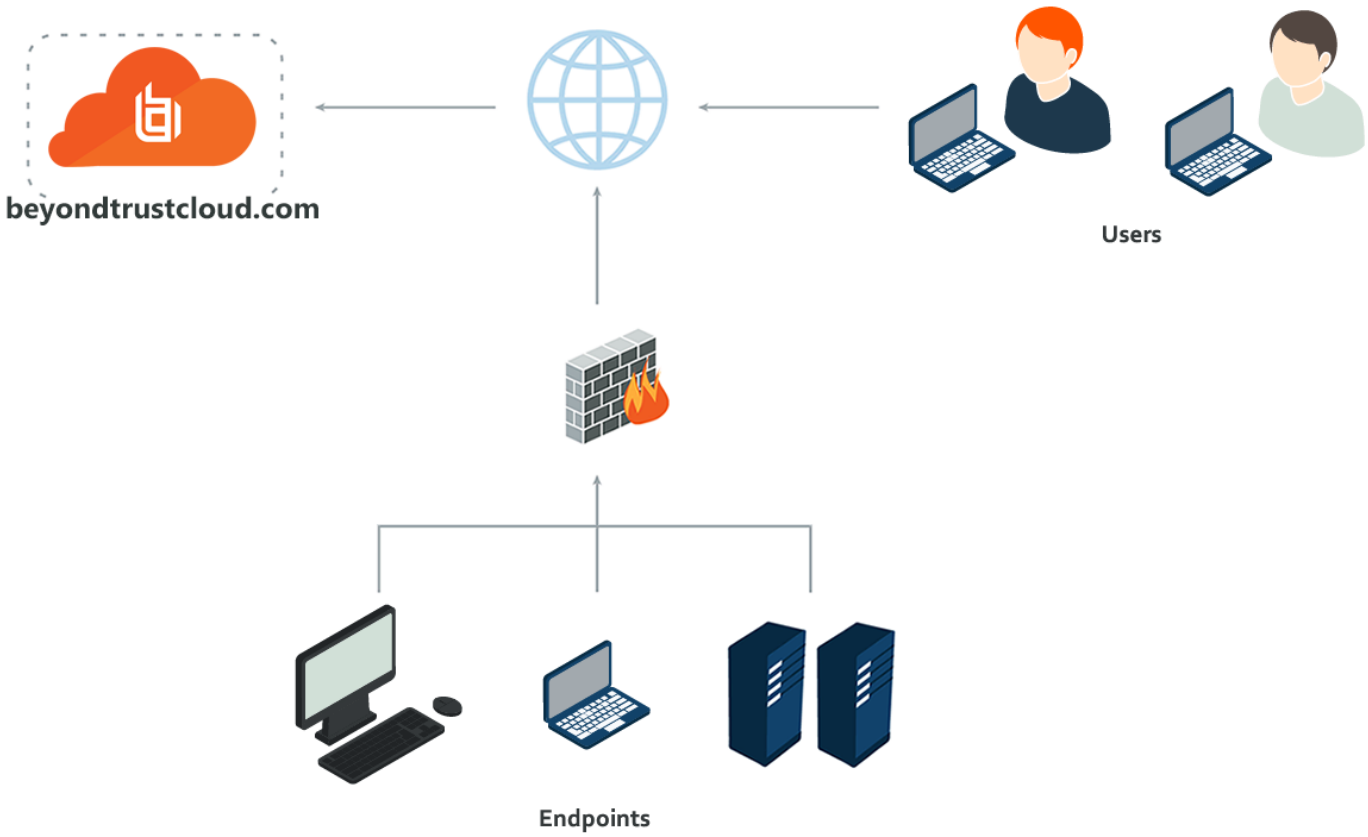
Review BeyondTrust Privileged Remote Access Cloud Network Infrastructure

The architecture of the BeyondTrust Privileged Remote Access application relies on the Privileged Remote Access cloud instance as a central routing point for all communications between application components. All sessions between users and remote systems occur through the server components that run on the B Series Appliance. To protect the security of the data in transit, Privileged Remote Access uses TLSv1.2 to encrypt all application communications.

Customers can configure the security features such that the Privileged Remote Access deployment complies with applicable corporate policies or regulations. Security features include role-based access control, secure password requirements, and a full audit trail.

Privileged Remote Access enables remote control by creating a remote outbound connection from the endpoint system to the Privileged Remote Access cloud instance. The cloud site is designed and tested to ensure it works properly and securely in the cloud infrastructure. Since all Privileged Remote Access sessions are initiated via outbound connections from the client to the B Series Appliance, it is possible to remotely control computers using Privileged Remote Access through firewalls.



Review BeyondTrust Appliance B Series Network Infrastructure

Each Privileged Remote Access cloud site comes with a subdomain of the BeyondTrust cloud DNS address, such as yoursite.beyondtrustcloud.com. If customers prefer to use their company web address with their own SSL certificate, they can use a

Canonical Name (CNAME) record to point the default site address to the preferred address.

Since this site accesses the /login interface, a simple yet descriptive name is the best practice. For example, a company named Smithson might use access.smithson.com for their CNAME record.

Review Sample Firewall Rules for Cloud Deployments

Below are example firewall rules for use with Privileged Remote Access Cloud, including port numbers, descriptions, and required rules.

Firewall Rules	
Internal Network to the PRA Cloud Instance	
TCP Port 443 (required)*	Used for all session traffic.
PRA Cloud Instance to the Internal Network	
TCP Port 25, 465, or 587 (optional)	Allows the B Series Appliance to send admin mail alerts. The port is set in SMTP configuration.
TCP Port 443 (optional)	B Series Appliance to web services for outbound events.

For information on setting Syslog over TLS, please see Appliance Administration: Set Syslog over TLS at https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/cloud/syslog-over-tls.htm. UDP/514 and/or TCP/514 for Syslog server on internal network is optional.

Use BeyondTrust Atlas in the Cloud

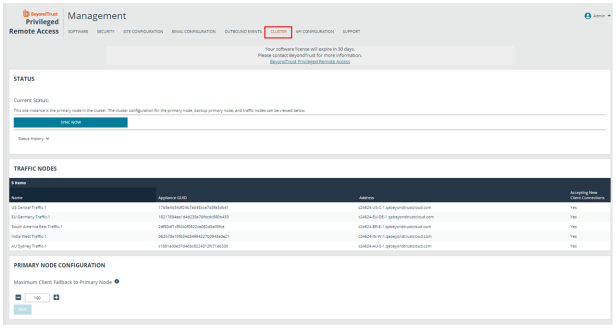
Similar to BeyondTrust Atlas Technology, Atlas in the Cloud is intended for large enterprise customers performing more concurrent sessions than can be effectively or efficiently handled by a single existing B Series Appliance model. This allows an organization to be effectively dispersed over different geographical locations and to access endpoints globally.

Creating a clustered BeyondTrust environment introduces new terminology: the primary and traffic node concept. The primary node serves as the main point of configuration for the site and also serves as the session initiation point of presence for the entire Privileged Remote Access site.

All configuration of the Privileged Remote Access site is handled on the primary node. Even though a cluster consists of multiple B Series Appliances, the /login administrative interface resides on the primary node and propagates most configuration settings to the traffic nodes automatically.

Note: *Atlas in the Cloud deployment is handled by BeyondTrust instead of the client.*

To access **Atlas in the Cloud** go to **/login > Management > Cluster**. From here you can view:



- **Current Status**: Confirms the role of the site instance from which you accessed the page.
- **Primary Node(s)**: Displays a list of the primary nodes available.
- **Traffic Nodes**: You can view traffic nodes, but you cannot add, edit, or delete them. You also cannot turn traffic nodes on or off. Traffic nodes use (customerID)-region.beyondtrustcloud.com for routing, which is controlled by the B Series Appliance, not the customer. Customers only control the primary node name/URL.
- **Maximum Client Fallback to Primary**: Allows the number of clients set to fall back to using the primary for traffic control if necessary.

While most of this page is read-only, you are able to perform a cluster data sync by clicking the **Sync Now** button. This ensures that the traffic nodes all have the same configuration.

For more information, please see the BeyondTrust Atlas Technology Overview at https://www.beyondtrust.com/docs/remote-support/how-to/atlas/wp-atlas-overview.htm.