The Privileged Remote Access Appliance in the Network

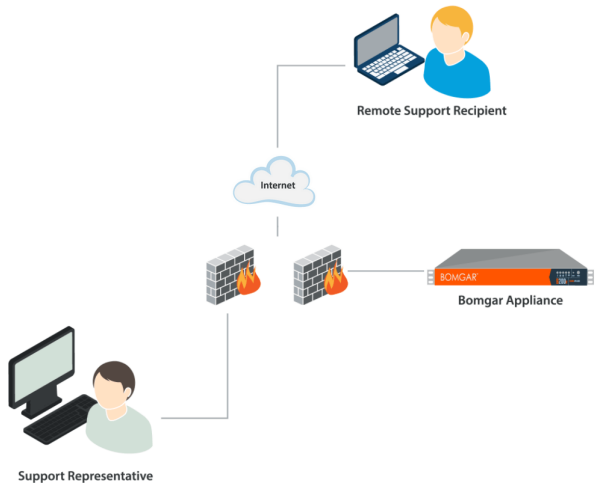
The architecture of the BeyondTrust application environment relies on the BeyondTrust Appliance as a centralized routing point for all communications between application components. All BeyondTrust sessions between users and remote systems occur through the server components that run on the appliance. To protect the security of the data in transit, BeyondTrust uses 256-bit Advanced Encryption Standard (AES) SSL to encrypt all application communications.

BeyondTrust's architecture offers customers the ability to choose how and where the appliance is deployed. Additionally, customers may configure the security features such that the BeyondTrust deployment complies with applicable corporate policies or regulations. Security features include role-based access control and secure password requirements.

BeyondTrust enables remote control by creating a remote outbound connection from the endpoint system to the BeyondTrust Appliance through firewalls. For BeyondTrust to provide remote control securely, the appliance is designed to use the most common network infrastructure or architecture that supports internet-accessible applications – a demilitarized zone (DMZ) with firewall protection.

The BeyondTrust Appliance is designed and tested to ensure it works properly and securely in internet environments. While the appliance can be deployed internal or external to your organization, to achieve optimal security, BeyondTrust recommends that you place the BeyondTrust Appliance inside the DMZ, as illustrated. This diagram shows the recommended configuration for one BeyondTrust Appliance.

By locating the appliance in the DMZ, the appliance is within the secure buffer zone. Since all BeyondTrust sessions are initiated via outbound connections from the client to the appliance, it is possible to remotely control computers using BeyondTrust through the firewalls.



Privileged Remote Access Appliance Network Infrastructure

DNS: Each BeyondTrust Appliance needs a physical connection to the network and a separate IP address. Additionally, a Domain Name System (DNS) record for each appliance is recommended, along with the DNS A Record or a Canonical Name (CNAME) record pointing to the appliance. The simple yet descriptive name is a useful approach. For instance, a company named 'Example' might use access.example.com for their DNS record.

Some companies have network standards and guidelines for DNS names that may increase the complexity of the site name. For instance, the 'Example' company might require every DNS name to include the geographical region and department within the name, such as usa.hr.example.com. This name is difficult to use and remember. In this instance, the best practice is to create a CNAME that ultimately points to the appliance and public site. The CNAME is usa.hr.example.com, as shown below:

access.example.com	CNAME	usa.hr.example.com
usa.hr.example.com	A	192.0.2.23

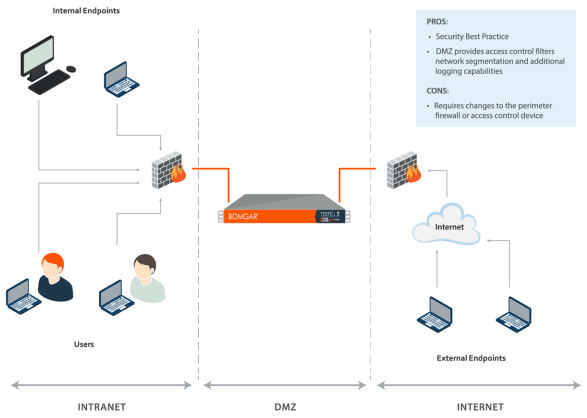
Here is one more example, using the common foo bar terminology:

foo.example.com	CNAME	bar.example.com
bar.example.com	A	192.0.2.23

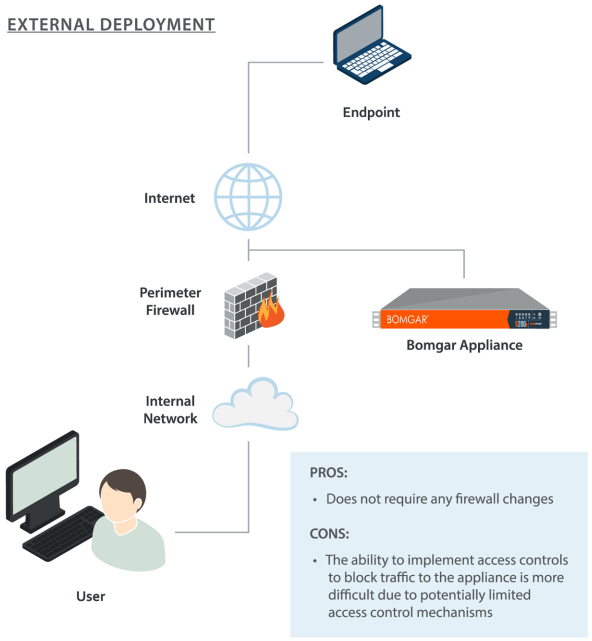
Deployment Options

DMZ Deployment (recommended): Deploying the appliance into a perimeter-based DMZ segment meets security best practice standards and is BeyondTrust's recommended location for the secure deployment of the device. A DMZ, or de-militarized zone, is a network that is protected by access control mechanisms. Access control may be provided by a firewall device, a router, or a switch that provides port and address filtering capabilities. The purpose of the DMZ is to limit access to systems that are deployed within it. In the case of the BeyondTrust Appliance, the DMZ will limit connectivity to the device and allow access only to the appropriate ports.

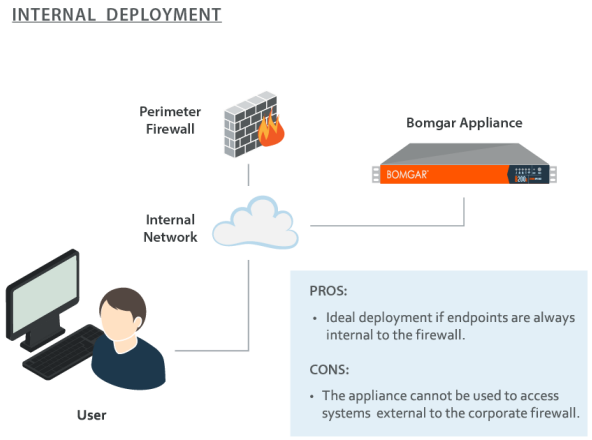
- For more information see "Example Firewall Rules Based on Privileged Remote Access Appliance Location" on page 4



External Deployment:In situations where a DMZ does not exist and is not possible due to technical or business constraints, the BeyondTrust Appliance may be deployed external to the perimeter firewall. The appliance consists of a hardened operating system and applications that are designed to be directly accessible.



Internal Deployment: Deploying the BeyondTrust Appliance on an internal network segment is ideal when the client base is completely internal or accessible through a VPN. No firewall changes are required because the device and all of the endpoint clients are internal to the firewall. In environments where the remote systems are external to the firewall, BeyondTrust recommends this deployment location only in the event that a DMZ does not exist or when the appliance cannot be deployed externally. An internal deployment of the appliance requires numerous changes to the environment and a solid understanding of perimeter firewall controls and Network Address Translation.



Example Firewall Rules Based on Privileged Remote Access Appliance Location

Below are example firewall rules for use with BeyondTrust, including port numbers, descriptions, and required rules. If an appliance has multiple IP addresses, outbound traffic for services such as LDAP can flow out of any configured address. Because of this, it is best practice to make firewall rules apply for all IP addresses configured on each BeyondTrust appliance.

Firewall Rules	
Internet to the DMZ	
TCP Port 443 (required)*	Used for all session traffic.
UDP Port 3478 (optional)	Used to enable Peer-to-Peer connections if the "Use Appliance as Peer-to-Peer Server" option is selected.
Internal Network to the DMZ	
TCP Port 161/UDP	Used for SNMP queries via IP configuration settings in the /appliance interface.
TCP Port 443 (required)*	Used for all session traffic.
DMZ to the Internet	
TCP Port 22 to the specific host **gwsupport.bomgar.com** (optional)	Default port used to establish connections with BeyondTrust Support for advanced troubleshooting/repairs. 443 may be used as an alternate port if needed.
TCP Port 443 to the specific host **update.bomgar.com** (optional)	You can optionally enable access from the appliance on port 443 to this host for automatic updates, or you can apply updates manually.
DMZ to the Internal Network	
UDP Port 123 (optional)	Access NTP server and sync the time.
LDAP - TCP/UDP 389 (optional)‡	Access LDAP server and authenticate users.
LDAP - TCP/UDP 636 (optional)‡	Access LDAP server and authenticate users via SSL.
Syslog - UDP 514 (required for logging)	Used to send syslog messages to a syslog server in the internal network. Alternatively, messages can be sent to a syslog server located within the DMZ.
DNS - UDP 53 (required if DNS server is outside the DMZ)	Access DNS server to verify that a DNS A record or CNAME record points to the appliance.
TCP Port 25, 465, or 587 (optional)	Allows the appliance to send admin mail alerts. The port is set in SMTP configuration.
TCP Port 443 (optional)	Appliance to web services for outbound events.
TCP Port 5832 (required if Passive Jump Client option is used)	Used as a listening port by Passive Jump Clients. Operating system firewalls should also be aware of this port. The port number is configurable by an administrator. This port is purely used for wakeup calls to the clients and is therefore not encrypted. After the client is woken, it launches the BeyondTrust session over an encrypted outbound TCP 443 connection.
TCP Port 5696	Allows the BeyondTrust PRA appliance to access the KMIP server located in the internal network for Data at Rest Encryption.

*Each of the following BeyondTrust components can be configured to connect on a port other than 443: access console, endpoint client, Jumpoint, connection agent.

‡ If the LDAP server is outside of the DMZ, the BeyondTrust Connection Agent is used to authenticate users via LDAP.

Network Considerations During Privileged Remote Access Appliance Install

The following questions should be considered when implementing your BeyondTrust Appliance in the network.

1. **How are connections established to the appliance?** The connection from each of the various clients is an outbound connection from the computer to the appliance, and the only required ports are 80 and 443. Therefore, the allowed ports would typically be 80 and 443 from the internet to the DMZ, and 80 and 443 from the internal network to the DMZ.
2. **Is port 443 the only port that needs to stay open inbound to the appliance?** The connection from each of the various clients is an outbound connection from the computer to the appliance, and the only required ports are 80 and 443. Therefore, the allowed ports would typically be 80 and 443 from the internet to the DMZ, and 80 and 443 from the internal network to the DMZ. Port 22 is an outbound port from the appliance to BeyondTrust. More ports may be available depending on your build.

   Optionally, the appliance can be configured to automatically check for updates from update.bomgar.com. This requires an outbound connection on port 443 from the appliance and the ability to connect to a DNS server to resolve this name. If the DNS server is within the DMZ, no additional ports would be required, but if the DNS server is in a different zone, the necessary ports for this would need to be allowed as described in the Firewall Rules table in the previous section. This can be avoided by downloading updates for the appliance and applying them manually. Lastly, the server is configured with an NTP server to sync the time on the appliance. This can be supported by connecting to clock.bomgar.com, or it can be supported pointing to an internal NTP server using Port 123.

3. **What other outbound connectivity does the appliance need?** The appliance can be configured with an NTP server to sync the time on the appliance. This can be supported by connecting to clock.bomgar.com, or it can be supported pointing to an internal NTP server using Port 123.
4. **Is the LDAP Server on the same LAN as your BeyondTrust Appliance?** If not, you must install a BeyondTrust Connection Agent on the LDAP server to support communications between the BeyondTrust Appliance and the LDAP Server.
5. **Will there be two appliances configured, one as a backup appliance to support automatic failover?** If so, the appliances need to be on the same subnet, and they each need a DNS A Record for their individual IP Addresses.
6. **Will you be utilizing a RADIUS Server with BeyondTrust?** If so, this is typically port 1812.
7. **Will you be utilizing a Kerberos Key Distribution Center (KDC) with BeyondTrust?** If so, the users typically communicate with their KDC over port 88 UDP.
8. **Is your client base completely internal or accessible through a VPN?** If so, deploying the BeyondTrust Appliance on an internal network segment is ideal, and no firewall changes are required, because both the appliance and all of the supported clients are internal to the firewall.
9. **Are you accessing endpoints outside of your company's internal network?** If so, best practices in network design discourage opening external access directly to your internal network. If you using BeyondTrust to access endpoints external to your network, it is highly recommended that the appliance reside in a DMZ that segments the internal network from the internet.
10. **How are updates to the appliance done?** The appliance can be configured to automatically check for updates from update.bomgar.com. This requires an outbound connection on port 443 from the appliance and the ability to connect to a DNS server to resolve this name. If the DNS Server is within the DMZ, no additional ports would be required, but if the DNS server is in a different zone, the necessary ports for this would need to be allowed. This can be avoided by downloading updates for the appliance and applying them manually.