BeyondTrust

Privileged Remote Access
The B Series Appliance and CJIS

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

TC:3/4/2024

Table of Contents

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

The BeyondTrust Appliance B Series and CJIS

BeyondTrust Privileged Remote Access is a comprehensive privileged access solution using an appliance-based architecture that can enable organizations to maintain and comply with Criminal Justice Information Services (CJIS) mandated policies. The BeyondTrust Appliance B Series gives users secure remote control of computers over the Internet or over the entire agency local networks.

Maintain Compliance

With BeyondTrust Privileged Remote Access, a user can see the device's screen and control the device's system remotely as if physically present, all while maintaining compliance. BeyondTrust Privileged Remote Access also enables streamlined third-party vendor access using a BeyondTrust Privileged Remote Access feature referred to as Access Invite. This enables agencies to eliminate requiring VPN access for outside vendors.

Access Systems

BeyondTrust Privileged Remote Access enables remote access to multiple operating systems, including Windows, Mac, and various Linux distributions. BeyondTrust Privileged Remote Access also enables remote control of various kinds of systems, including laptops, desktops, servers, kiosks, point-of-sale systems, and network devices.

Access Anywhere

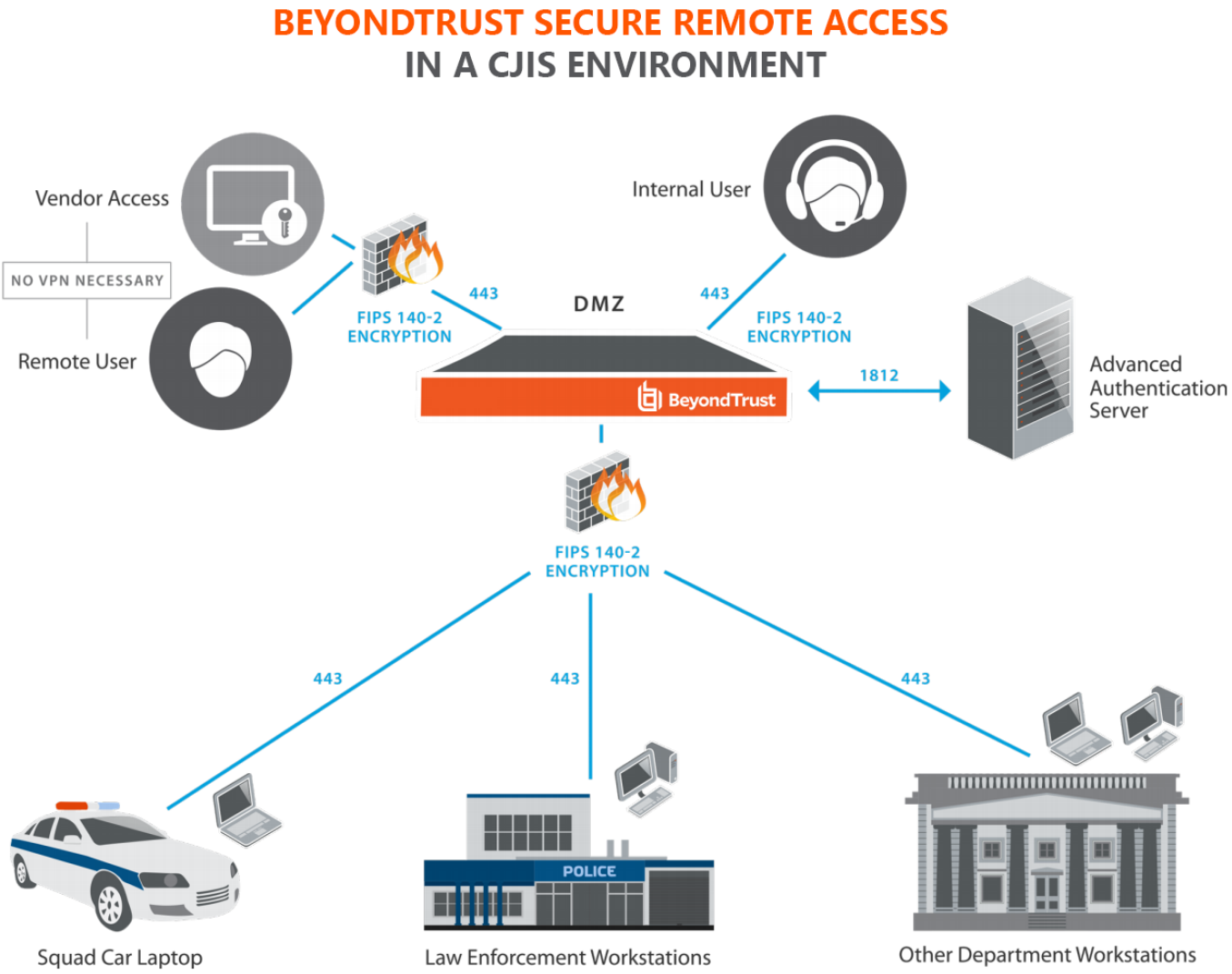
BeyondTrust Privileged Remote Access can work over internal and extended networks, or it can be Internet accessible. BeyondTrust Privileged Remote Access mediates connections between users and endpoints, allowing screen-sharing, remote control, file downloads/uploads, and access to system information and diagnostics.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

BeyondTrust Privileged Remote Access Architecture

Using multiple features designed to ensure the security of remote access sessions, BeyondTrust Privileged Remote Access integrates with existing advanced authentication identity management systems. This assists agencies in securing sensitive data by making sure that the users accessing endpoints have been validated properly. BeyondTrust Privileged Remote Access also adds a layer of additional auditing capabilities via detailed session logs and video recordings of every access session conducted. BeyondTrust Privileged Remote Access sessions are also encrypted in transmission using FIPS 140-2 compliant algorithms. The Access Invite functionality can be carried out impromptu, removing the need to create a service account over a FIPS-compliant VPN. An invited outside user is actively monitored and controlled by an internal agency user for the duration of the access session.

The following diagram was taken from the CJIS security policy and depicts where BeyondTrust Privileged Remote Access would fit into a conceptual topology diagram for a law enforcement agency:



©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

In the diagram above BeyondTrust Privileged Remote Access would be located in the agency's DMZ. BeyondTrust Privileged Remote Access uses the advanced authentication server to validate all users/vendors. When accessing any end systems the session traffic is encrypted using FIPS-compliant encryption. BeyondTrust Privileged Remote Access can be used to securely access all agency systems that are internal as well as external to the agency network. Also depicted in the diagram is the BeyondTrust Privileged Remote Access Access Invite feature. This BeyondTrust-specific functionality is applied to a third-party vendor coming in via the Internet, without requiring a VPN connection. This connection is also FIPS-compliant encrypted. The same concept can also be extended to employees who need to access internal systems while working remotely.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Authentication to the BeyondTrust Appliance B Series

BeyondTrust Privileged Remote Access may be provisioned for locally-defined BeyondTrust Privileged Remote Access user accounts, or can be integrated into existing authentication sources. For instance, a commonly integrated authentication source is RADIUS which enables agencies to leverage their existing advanced authentication server. When using a directory such as this, all authentication follows the existing controls and processes in place for safeguarding user accounts.

Additional security providers are available that allow for user authentication using SAML, Kerberos, or LDAP. Each of these providers can be configured to use LDAP groups to set the users' permissions, allowing you to map existing LDAP groups to users in BeyondTrust Privileged Remote Access.

There are a large number of granular permissions that can be granted to users. These permissions determine what features in BeyondTrust Privileged Remote Access a user has access to.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

SSL/TLS in the BeyondTrust Appliance B Series

BeyondTrust Privileged Remote Access can be configured such that it enforces the use of SSL for every connection made to the B Series Appliance. BeyondTrust Privileged Remote Access requires that the SSL certificate being used to encrypt the transport is valid, and also can be configured to ensure that only FIPS 140-2 compliant algorithms are used.

BeyondTrust Privileged Remote Access can natively generate CSR request using RSA 2048, 3072, or 4096 bit RSA key length choices or ECDSA keys using P-256 or P-384 curves, but also supports importing certificates generated off of the B Series Appliance. Available cipher suites can be enabled or disabled and re-ordered in the preferred preference of use. The BeyondTrust Privileged Remote Access software itself is also uniquely built for each customer and a unique encrypted license file is created that ensures all BeyondTrust Privileged Remote Access clients are only valid for the site in which they are built. Additionally, customer SSL certificates are built into the license file and must match the certificates being used on the B Series Appliance.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Validation of the BeyondTrust Appliance B Series

To ensure the security and value of our product, BeyondTrust Privileged Remote Access incorporates vulnerability scanning in our software testing process. We track the results of vulnerability scans performed prior to a software release and prioritize resolution based on severity and criticality of any issues uncovered.

Should a critical or high-risk vulnerability surface after a software release, a subsequent maintenance version release addresses the vulnerability. Updated maintenance versions are distributed to our customers via the update manager interface within the BeyondTrust Privileged Remote Access administrative interface. Where necessary, BeyondTrust Technical Support will contact customers directly, describing special procedures to follow to obtain an updated maintenance version.

Currently BeyondTrust Privileged Remote Access conducts internal vulnerability assessments using tools from IBM Rational App Scan.

BeyondTrust offers distinct products that have successfully undergone FIPS 140-2 Level 2 certification. In order to receive this certification the BeyondTrust Secure Remote Access software and the physical BeyondTrust Secure Remote Access hardware passed a very stringent review conducted by the National Institute of Standards and Technology.

- Current FIPS Certified Software Version: 16.2.1 FIPS
- Current FIPS Certified Firmware Version: 4.4.2 FIPS
- NIST Certification for the BeyondTrust Cryptographic Engine algorithms:

AES	Cert. #4767
CVL	Certs. #1411 and #1546
DRBG	Cert. #1648
ECDSA	Cert. #1196
HMAC	Cert. #3180
KTS	AES Cert. #4767 and HMAC Cert. #3180; key establishment methodology provides 128 or 256 bits of encryption strength
RSA	Cert. #2608
SHS	Cert. #3912

All B Series Appliances running Base software versions 5.3.0 – 5.5.0, including the PRA Virtual Appliance and Cloud Appliance, make use of the same FIPS-validated version of the BeyondTrust Secure Remote Access Cryptographic Engine that is available in the FIPS-validated B Series Appliances. The BeyondTrust Secure Remote Access Cryptographic Engine also supports additional, non-FIPS validated algorithms in order to support a broader array of potential encryption requirements.

All of the encryption algorithms included with a B Series Appliance can be enabled or disabled at your discretion.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Audit Privileged Remote Access Sessions

BeyondTrust Privileged Remote Access provides two types of access session logging. All the events of an individual access session are logged to a text-based log. This log includes users involved, system information, and any other actions taken by the BeyondTrust Privileged Remote Access user. This data is available on the B Series Appliance in an un-editable format for 90 days, but can be moved to an external database using the BeyondTrust Privileged Remote Access Integration Client (IC). All sessions are assigned a unique **session id** referred to as an LSID. The LSID is a 32 character string that is a unique GUID for each session, and is stored as part of each session log for every session conducted.

BeyondTrust Privileged Remote Access also allows the ability to enable session recordings. This records the GUI of the endpoint's screen for the entire access session. This recording contains metadata to identify who is in control of the mouse and keyboard at any given time during the playback of the recorded session. The period of time these recordings remain available is dependent on the amount of session activity, and the available storage. As with the access session logging, these recordings can be moved to an external file store using the BeyondTrust Privileged Remote Access IC.

Each BeyondTrust Appliance B Series model has differing amounts of available disk space, and by default is set to purge data over 90 days old. The BeyondTrust Privileged Remote Access IC can be used to export data from the B Series Appliance and store it externally if needed to comply with security policies.

The Integration Client is a Windows application used to export reports, recordings, and backups from one or more B Series Appliances according to a defined periodic schedule. The IC uses plug-in modules to determine the repository for the exported data. BeyondTrust Privileged Remote Access provides two IC plug-in modules. One handles export of reports and video recordings to a file system destination. The second exports select report information (a subset of the entire data collection) to a Microsoft SQL Server database. Setup of the IC for SQL Server includes all of the procedures needed to automatically define the necessary database, tables, and fields.

In practice, the Integration Client is used to export access session data that must be retained for legal and compliance reasons. The reports and recordings are archived in a file system, indexed by the B Series Appliance and session ID. Data stored in the SQL Server tables may be queried to locate the BeyondTrust Privileged Remote Access session ID corresponding to given search criteria such as date, user, or IP address.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.