



Directory Bastion

www.clearswift.com



www.eb2bcom.com

Directory Bastion is a specialised stand-alone product, which is a new addition to the Clearswift Bastion product family. Its purpose is to allow X.500 Directory data to be synchronised between two X.500 Directory System Agents (DSAs) on two otherwise disjoint networks, whilst maintaining an assured separation between the two networks it interconnects.

The Directory Bastion ensures that the only communication that it allows to traverse between the two networks conforms to the Directory Information Shadowing Protocol (DISP, defined in ITU-T Rec. X.525) between explicitly identified DSAs. Because DISP is the standard protocol to synchronise directory data between DSAs, a Directory Bastion can be inserted between two DSAs without requiring anything other than normal shadowing agreement configuration on the DSAs. Apart from network level addressing, the Directory Bastion is entirely transparent to the DSAs.

The Directory Bastion builds on the existing Bastion product, and the ITSEC E3/Common Criteria EAL4 evaluated component of Bastion is unchanged in Directory Bastion. A proxy supporting the Remote Operations Service Element (ROSE), which supports all X.500 protocols, replaces each (unevaluated) X.400 or SMTP Proxy. This ROSE Proxy consists of relatively small interface additions to existing highly stable software that has been deployed in the Clearswift Route400 P7 client and server products for more than eight years. In addition, a new version of the existing VETASN program (that verifies X.400 P1 protocol) will be created. This will operate within a DMZ compartment (see UBA SDD Part 1) in each direction of data flow to verify that the protocol is DISP, and that the source and destination match configured values. Figure 1 illustrates this.

The Directory Bastion is based on DISP for four reasons:

- DISP is the standard protocol for replicating Directory data between DSAs, and therefore the Directory Bastion can be inserted between any two DSAs (potentially from two different vendors) without requiring any software changes to the DSAs.
- DISP identifies the source and destination DSAs within the ROSE protocol to enable filtering to be applied differently between different DSA pairs if required.
- DISP supports all features of X.500, including signed attributes.
- DISP fully defines incremental updates, allowing propagation of only data that has changed.

Furthermore, Clearswift considered that it is easier to evaluate a filter on an ASN.1 protocol (DISP) than a filter on a text-based protocol (e.g. LDIF) because it is much easier for an attacker to place an attack on the filter in text than in ASN.1, as the ASN.1 must parse correctly before the filter code is activated.

Canberra: 02-6234-8043

Melbourne: 03-9831-6666

Sydney: 02-9238-2005

Email: sales@eb2b.com.au

Web: www.eb2b.com.au