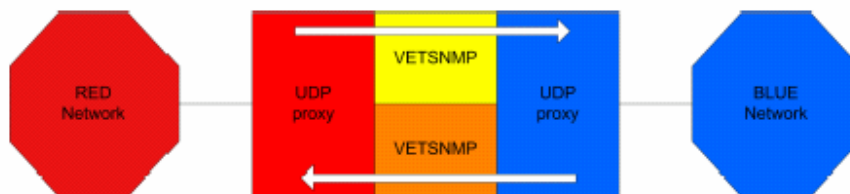




## SNMP Bastion

CS Bastion™ II V2.1 (CSB2.1) is a generic framework that provides an application level firewall between sensitive networks. CSB2.1 can be configured to support a variety of different protocols by using different 'proxies' to manage each subscriber network interface. One proxy option is referred to as the UDP proxy, which enables CSB2.1 to relay protocols that use UDP as a transport protocol between subscriber networks. VETSNMP supplements the UDP proxies by sitting between the proxies and ensuring that only audited and policed SNMP traffic can flow in each direction. These components are not security critical components of CSB2.1 and can be upgraded without impacting the CSB2.1CC/EAL4 certified configuration.

Figure 1-1 shows CSB2.1 in SNMP configuration. This configuration is commonly referred to as *SNMP Bastion*.



*Figure 1-1 SNMP Bastion*

As can be seen in Figure 1-1, SNMP Bastion includes two UDP proxies and two VETSNMP utilities. These four components are known as the SNMP Bastion subsystems and are separated by CSB2.1 internal interfaces. All traffic flow across the CSB2.1 internal interfaces are UDP datagrams stored as binary ASN.1-encoded files.

SNMP Bastion thus enables communication between Simple Network Management Protocol (SNMP) Management Stations on one network and SNMP Managed Devices on the other network where assured network separation between these networks must be preserved.

SNMP Bastion ensures that the only communication that can pass through it from one network to the other is SNMP V1 and V2c. SNMP Bastion also controls which operations in the SNMP protocol are permitted in each direction of message flow. It ensures that only devices for which it is configured may communicate through it, and also controls which SNMP Management Information Bases (MIBs) are permitted between these devices.

SNMP Bastion architecture requires that the IP address of each external system that is to communicate through it must be configured into a Trusted Solaris network family. Furthermore, SNMP does not contain names or addresses within the protocol but instead relies on IP packet addresses to identify Management Stations and Managed Devices. Ideally, SNMP Bastion would preserve the IP addresses of each external system. However, this would require the address of each RED network system to be both the address of an

external system in the RED network family and an address of the Bastion itself in the BLUE network family, and vice versa for BLUE network systems. Trusted Solaris will not permit one address to be in two disjoint network families. Therefore SNMP Bastion must itself use an alternative address when it represents each external system. This alternative address is termed the ghost address for each external system.

In Figure 2-1, on the RED network each Management Station is identified by its real address and on the BLUE network it is identified by its ghost address. Similarly, on the BLUE network, each Managed Device is identified by its real address and on the RED network it is identified by its ghost address. In this configuration, the ghost addresses for Managed Devices form a ghost network on the RED network, and the ghost addresses for Management Stations form a ghost network on the BLUE network.

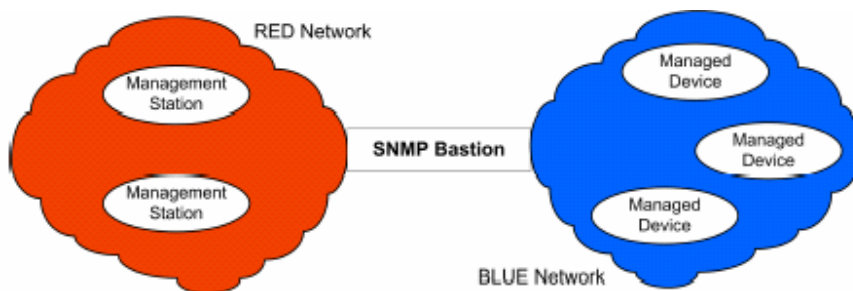


Figure 2-1 SNMP Bastion deployment environment

Where it is desirable that real addresses for Managed Devices are displayed by Management Stations, SNMP Bastion may be used in series with a packet firewall that provides Network Address Translation (NAT), as shown in Figure 2-2.

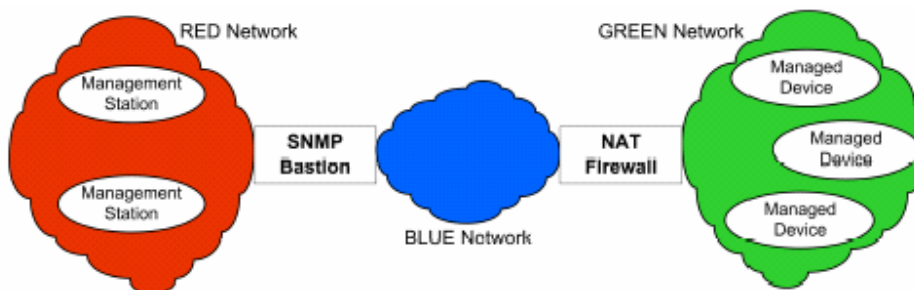


Figure 2-2 SNMP Bastion with NAT firewall

Here each Management Station and Managed Device is identified by its real address on both the RED and GREEN networks, and by an alias address on the BLUE network. In some environments, it may be desirable for this packet firewall to be evaluated too, in order that a higher overall assurance of network separation is provided using *defence in depth*.

The SNMP Bastion subsystems run on CS Bastion II V2.1 (CSB2.1) which in turn runs on Trusted Solaris 8 12/02 (TSOL8). To administer the SNMP Bastion subsystems you require direct access to the workstation running TSOL8, including a TSOL8 login account, password and access to (at least) the CSB2.1 "cots" role. If you are the sole Bastion Administrator you will adopt the default `csbuser` account (see the CSB2.1 *Administration Guide*) on delivery of your system, otherwise you must ask an existing Bastion Administrator to set you up a new user account.

An SNMP Bastion has the CSB2.1 archiving function disabled, and assumes no additional CSB2.1 subsystems are installed. Therefore, exactly four CSB2.1 compartments are occupied, as listed in Table 4-1.

Table 4-1 SNMP subsystems in CSB2.1 compartments.

SNMP Subsystem	CSB2.1 compartment	Colour of compartment
UDP Proxy <i>managing RED network</i>	MTA1	Red
UDP Proxy <i>managing BLUE network</i>	MTA2	Blue
VETSNMP utility <i>managing RED to BLUE flow</i>	VET11	Yellow
VETSNMP utility <i>managing BLUE to RED flow</i>	VET21	Orange

The SNMP Bastion subsystems are installed and part-configured for a customer as part of product delivery. Unlike many other CSB2.1 variants, the SNMPBastion subsystems are relatively closely coupled, and are configured using a common configuration utility.

### About eB2Bcom

eB2Bcom is an innovative Australian owned company specialising in the distribution, implementation and support of best-of-breed products for Identity Management, Security, MetaDirectory infrastructure & applications, Telecommunications, and ISP Messaging and solutions for Defence, Police, Intelligence & Enforcement. An experienced team of software engineers are available for consulting in and around X.500/LDAP directories. These services including:-

- X.500, X.509 and LDAP architectural consulting and design of directory and security solutions.
- X.500 schema and basic access control design and implementation.
- Interface design and implementation for directory centric solutions



**Sydney:** +61-2-9779-1597  
**Melbourne:** +61-3 -9896-7800  
**Brisbane:** +61-7-3871-1440  
**Singapore:** +65-6841-7374  
**email:** [sales@eb2bcom.com](mailto:sales@eb2bcom.com)  
**Web:** [www.view500.com](http://www.view500.com) or [www.eb2bcom.com](http://www.eb2bcom.com)