Software Product Description

PRODUCT NAME: DIGITAL Remote Access Security Version 2.2 **SPD 56.19.01**

DESCRIPTION

DIGITAL Remote Access Security (DRAS) is an application that allows you to configure and manage secure remote access to your network. DRAS controls which users can access the network, when users can access the network, and what users can do when connected to the network. DRAS also provides accounting capabilities to track users' activities.

The DRAS software uses the Remote Authentication Dial-In User Service (RADIUS) protocol as defined in the current Internet Engineering Task Force (IETF) RFC 2138 and RFC 2139. Any network access server that communicates with the DRAS server needs to support the RADIUS protocol.

The DRAS V2.2 features described in this document are fully supported when the DRAS server is used in combination with DECserver network access severs running DECserver Network Access Software V2.2, which includes a fully compatible RADIUS client. Network access servers from other vendors may also support RADIUS clients and may work with DRAS, but interoperability is not guaranteed nor support implied.

Components

The DRAS product has two major components: the DRAS Server and the DRAS Manager.

The DRAS Server is the application that communicates with various clients that send it access requests. A client can be a network access server (NAS) or a remote management workstation.

The DRAS Server stores information about groups, users, clients, sessions, and authentication methods as objects in a local database. Objects include:

- All RADIUS clients that send authentication, authorization, and accounting requests to the DRAS server.
- All remote management stations that are authorized to access the DRAS Server's database.
- All users for whom the DRAS Server performs authentication. Users do not interact directly with the DRAS Server, but with a RADIUS client that then sends the authentication requests to the DRAS Server.
- All administrative users that are authorized to access the DRAS Server's database for management purposes.

The DRAS Manager is the Windows-based graphical user interface application that is used to manage the DRAS Server and to configure its database. The DRAS Manager can:

- Stop, pause, and resume a remote or local DRAS Server
- View status of local or remote servers
- Manage objects in the local or remote DRAS Server databases

Services and Features

The DRAS Server provides the following services to its clients:

Service	Description
Authentication	Allows the NAS to identify an external user requesting network access correctly and reliably
Authorization	Defines what services the user may access on the network
Accounting	Provides information about services used by the user for billing, audit trail, and troubleshooting purposes

The DRAS Server supports the following *authentication* methods:

- **CHAP**—Static password authentication using PPP's Challenge Handshake Authentication Protocol.
- **DEFENDER**—AssureNet Pathway's challenge/response two factor authentication. It uses the DES algorithm to generate unique one-time passwords.
- **HOST**—DRAS Server host login authentication.
- **OTP**—An MD5-based challenge/response authentication. It implements one-time password authentication and is derived from Bellcore's S/key.
- **PASSWORD (PAP)**—The DRAS Server uses a static password, in conjunction with a user name, registered in its database for the user. Typically, the user can change this password.
- **SECURID**—Security Dynamics Technologies' SecurID token card one-time passcode authentication. You need an SDI ACE/Server on the network for this authentication method.
- **WATCHWORD**—RACAL-Guardata's challenge/response authentication. It uses the encryption algorithm that the Watchword calculator implements.

The DRAS Server supports the following criteria for *authorization*:

Criteria	Description
User account enabled	The DRAS Server checks the user object in its database to determine whether the user account is enabled. User objects are likely to be disabled following break-in detection or a configurable amount of time during which the object is not used.
User account expiration	The DRAS Server checks the user expiration date and time in the user database against the current local time.
User account access hours	The DRAS Server checks the user access hours, which define a weekly access schedule, against the local time.
User group check	The DRAS Server checks group objects in its database against the following criteria: group enabled, group expiration, group access hours.

The DRAS Server supports the following security facilities:

- Break-in detection—The DRAS Server can detect and track consecutive authentication failures for a particular user. When consecutive authentication failures occur, the DRAS Server disables the user account. Enabling requires manual intervention. The DRAS Server can also detect and track consecutive authentication failures from a particular port/NAS. When consecutive failures occur in this way, the DRAS Server rejects any further requests from this port on the NAS and puts the port/NAS on a blacklist.
- Duress login detection—Certain authentication devices allow a user under a threat to connect and tell the NAS that the connection is occurring under abnormal conditions. When detecting this, the NAS must allow the connections but tracks, flags, and possibly reports the exception to the management station. This detection depends on the capabilities of the authentication method in use.

The DRAS Server collects *accounting* and event information about the DRAS Server operation and connection activity. The DRAS Server stores this information in its accounting database. The information in the accounting log file can be displayed or exported as a common delimited text file to be printed or imported into another application.

HARDWARE REQUIREMENTS

DRAS Server Software

The DIGITAL Remote Access Security server software runs on the following systems:

- DIGITAL Alpha Systems
- DIGITAL VAX systems
- Intel PCs

Server Software Disk Space Requirements

To install and operate the DIGITAL Remote Access Security server software, you need the following minimum disk space:

For OpenVMS VAX server	1400 disk blocks
For OpenVMS Alpha server	2100 disk blocks
For DIGITAL UNIX server on Alpha	2 MB
For Windows NT server on Alpha	7 MB
For Windows NT server on Intel PCs	4 MB

Management Utility Software Disk Space Requirements

To install and operate the DIGITAL Remote Access Security management utility software, you need the following minimum disk space:

For Windows NT management utility on Alpha	4 MB
For Windows NT management utility on Intel PCs	2 MB
For Windows 95 management utility on Intel PCs	2 MB

SOFTWARE REQUIREMENTS

DRAS Server Software

The DIGITAL Remote Access Security server software runs in the following operating system environments:

- OpenVMS Alpha Version 6.2 or greater
- OpenVMS VAX Version 6.1 or greater
- DIGITAL UNIX Version 3.2 or greater
- Windows NT Version 3.51 or greater

DRAS Management Utility Software

The DIGITAL Remote Access Security management utility software runs in the following operating system environments:

- Windows NT Version 3.51 or Windows NT Version 4.0
- Windows 95

GROWTH CONSIDERATIONS

The minimum hardware and software requirements for any future versions of this product may differ from the requirements of the current version.

DISTRIBUTION MEDIA

CD-ROM distribution only

DOCUMENTATION

- CD-ROM distribution
- Hardcopy documents (optional)

PRODUCT ORDERING INFORMATION

Description	Order Number
DIGITAL Remote Access Security all-platform CD-ROM license and media kit	QB-55FAA-SA
DIGITAL Remote Access Security Loan	QB-55FAA-LD
Documentation kit	QB-55FAA-GZ

® Defender is a registered trademark of AssureNet Pathways, Inc.

® Intel is a registered trademark of Intel Corporation.

® SecurID is a registered trademark of Security Dynamics Technologies, Inc.

® S/Key is a registered trademark of Bell Communications Research, Inc.

® UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Ltd.

® Windows 95 is a registered trademark of Microsoft Corporation.

™ WatchWord is a trademark of Racal-Guardata, Inc.

™ Windows NT is a trademark of Microsoft Corporation.

™ The DIGITAL logo, DECserver, DIGITAL, DIGITAL Alpha Systems, OpenVMS, and VAX are trademarks of Digital Equipment Corporation.

All other trademarks and registered trademarks are the property of their respective holders.