NEXSION

NXSecure

Highlights

User Identification

User Authentication

Access Control

Availability

Reliability

Scability

Security

NX/Secure offers a suite of SSL (Secure Socket Layer) products. These products secure access for web pages, Pathway server classes, OLTP Sysem transactions and management screens, and Web Services when used in conjunction with the SOAPTP product range. Users can be authenticated using their Guardian User ID and Password, and via X.509 certificates. This allows NX/Secure users to be sure that their valuable NonStop data is secure regardless of the access mechanism.

NX/Secure improves HP NonStop user security by providing an access control system that addresses these basic requirements:

- User Identification -A form of credential is obtained from the user to identify them. This might be a simple User ID and password, a digital certificate or some sort of token such as an RSA SecurID token.

- User authentication determines that the supplied credentials match the "master" credentials.

- Resource Access Authorization -Determines if the user is authorized to access the resource. This step requires the name of the resource and the action the user is attempting. The access control system is flexible enough to allow a wide range of resource and potential actions to be specified.

NX/Secure addresses the standard requirements for an access control system as well as the HP NonStop basics of availability, scalability, and reliability. As a NonStop Guardian application, it provides an ideal environment in which to reliably secure enterprise applications such as those generally hosted on the HP NonStop Server.

NX/Secure provides tighter security to the authorization given to any authenticated user. To corporations needing to protect their HP NonStop Server it offers a way to ensure that only the right users have access to the right information and resources. Additional benefits include the following:

- Enhanced security for any NonStop application; Secure web access including web pages, Pathway and BASE24 applications, and web services;

- Extensive configuration support options that allow all resources, actions, identifiers, authenticators and authorizors to be configured;

“f knowledge can create problems,
it is not through ignorance that we can solve them.
Isaac Asimov (1920 - 1992)”

NXSecure

- An audit trail logs command and control events and, optionally, authentication and authorization attempts.

Two fundamental elements in addressing network security include authentication and privacy. Authentication is permissive in nature, concerned with user identity and whether a particular user ought to have access to a particular file. Privacy, as related to network security, refers to the obfuscation of the data flow between the user and the host such that it may not be intercepted by any covert third party with potentially malicious intent.

NX/Secure supports these capabilities using open published standards. HP NonStop users now have security solution that allows for secure interoperability across disparate systems. Supported standards include:

1) Secure Socket Layer / Transport Level Security (SSL/TLS). The SSL / TLS standard is a broadly recognized and supported standard delineated in RFCs 3546, 3268, and 2818.

2) Certificate Authority (CA). The use of a trusted entity to provide digital certificates is a widely used standard to verify that clients and servers are who they claim to be. It, through the X.509 Public Key Infrastructure (PKI), has been documented in memos RFC 3631, 3280, and 1421-1424.

NX/Secure is compatible with any existing Guardian application. It can authenticate users against a range of "authenticators", including BASE24, application databases, Guardian user-id / password information and host certificate stores. In this manner it protects HP NonStop platform resources against unauthorized access. It may interface with any application that uses socket-based TCP/IP connectivity.

NX/Secure's authentication capabilities ensure that each end of a secure connection has a valid certificate issued by a trusted third party. Our software verifies the certificate owner and handles authorization to identify the certificate holder and the exact web service to invoke and access. NX/Secure supports authentication on Guardian User ID and password, X.509 Certificate, application user information and more.

Once the user is authenticated, NX/Secure will authorize it to run only those applications to which it should have access.