NONSTOP SERVER SECURITY TECHNICAL UPDATE

Wendy Bartlett
Distinguished Technologist, HP
24 August 2011

AGENDA

- New and upcoming NonStop OS security capabilities
- Safeguard and OSS enhancements
- SQL/MX enhancements
- iTP Secure WebServer enhancements

NEW NONSTOP OS SECURITY CAPABILITIES

- NonStop OS security update bundle:
  - NonStop SSH and SFTP
  - NonStop SSL
  - XYGATE Merged Audit
- NonStop SFTP API
- XYGATE Compliance PRO

NonStop OS Security Update Bundle

- New Security package introduced in 2010.
- Delivers three security products as part of the basic OS software suite.
  - Provided with the OS on new system orders
  - Available to installed J Series or H Series servers for a small upgrade fee.
  - Same products must be purchased separately for G Series platforms
- Includes the following products:
  - NonStop SSH
  - NonStop SSL
  - XYGATE Merged Audit
- Brought to the market through a business relationship with two of our Security partners.

comforte®

XYPRO

Enhancement Add-ons to the Security bundle

Data in Motion Security

NonStop SSH

Available now!

SFTP API Plug-in

We now offer an API for SFTP so applications which call FTP today can be pointed to SFTP easily without major coding work.

XYGATE Merged Audit

Available now!

Base24 Plug-in

We offer a plug-in for Merged Audit that allows you to gather events from ACI Base24 logs as part of your reporting.

Coming soon!

HLR Plug-in

New plug-in will allow Telco customers to gather events from HLR (Home Location Registry) logs as part of reporting.

Audit Reporting and Alerts

This is a rolling (up to three year) Statement of Direction and is subject to change without notice

NonStop SSH - SFTP API Plug-in

New API plug-in for NonStop SSH allows customer applications to programmatically access SFTP the same way they previously accessed FTP.

- Provides a secure file transfer capability using SSH.
- No coldload required to install and use.
- Requires prior purchase of NonStop SSH from HP, either by having purchased the independent product or as part of the OS Security Upgrade bundle.
- A license file enables the functionality for use by your application.

XYGATE Compliance PRO

Can my system pass a compliance audit?

XYGATE Compliance PRO is a sophisticated and powerful tool specifically designed for the NonStop platform to help customers:

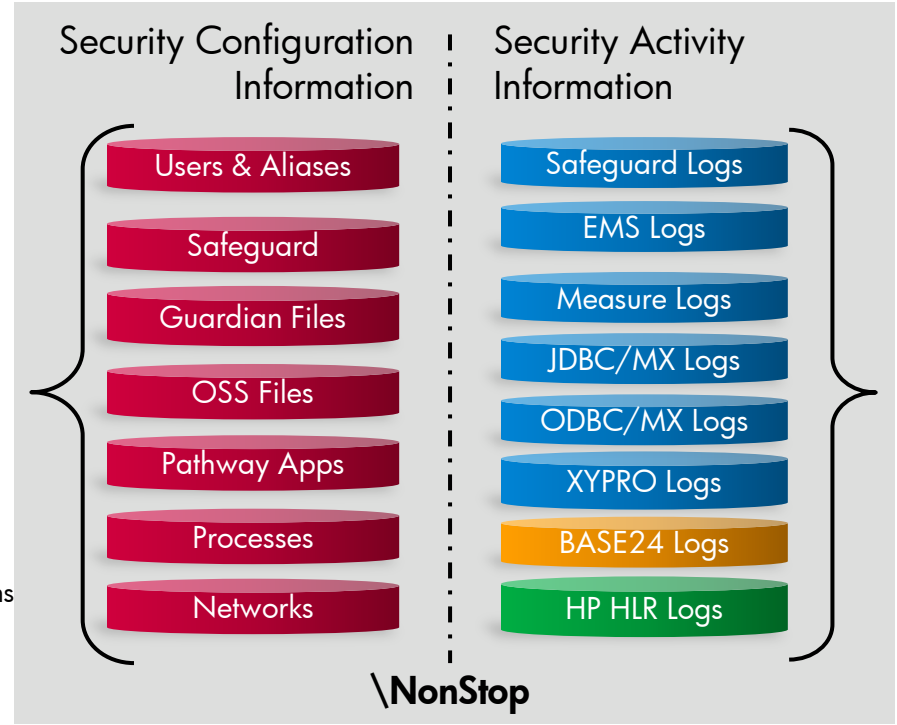
- analyze system security settings and configurations
- gather extensive system data to compare changes in the system from different points in time
- modify their security settings to improve protection of their system
- have confidence about monitoring compliance with documented evidence
- available as an independent product, ships on a CD

Compliance PRO vs. Merged Audit

XYGATE Compliance PRO

How is the system secured?

- **Examine for compliance**
  - Compare system configuration & security settings against:
    - Regulations
    - PCI/DSS, SOX, HIPAA, etc
    - Best practices
    - Internal security policies
  - Review recommendations
  - Stay up to date with latest standards
- **Integrity Checking**
  - Compare files
  - Compare entire systems
- **Access Mapping**
  - Examine what users access
  - Compare access across systems
- **Extensive Reporting**
  - Prove compliance to Auditors & Senior Management



XYGATE Merged Audit

What is happening on the system?

- **Consolidate Audit Logs**
  - Gather from NonStop audit sources across the entire NonStop network
  - Filter to include only what you need
  - Run detailed canned reports
  - Customize reports to meet your needs
- **Receive Alerts**
  - EMS
  - Send to eMail or Pager
  - Security Event Display includes visual and auditory alerts
- **Enterprise Security**
  - Deliver NonStop audit data to SIEM solutions (like ArcSight)
  - Integrate NonStop data into the Enterprise Security Architecture

UPCOMING NONSTOP OS SECURITY CAPABILITIES

- XYGATE User Authentication
- XYGATE Access Control

Authentication

- The NonStop OS provides unique identification for users via Guardian user IDs and Safeguard aliases, both with 64 character strong password support
- It does not:
  - Consult enterprise authentication solutions
  - Support multi-factor authentication
  - Consider external factors
  - Provide flexible controls over group managers

XYGATE User Authentication – future offering!

Features

XYGATE User Authentication, available in the future from HP, allows customers to implement logon controls at a granular level and integrate their NonStop server into larger LDAP environments

- Logon Controls at a granular level, including time based.
- Rules for User group logons and controls for group manager capabilities
- Audit reporting on logon events
- IP, Requestor and Ancestor controls
- LDAP interface for NonStop
- Support for RSA SecurID tokens and RADIUS authentication
- Will be available as an independent product shipped on a CD for J Series, H Series and G Series.

XYGATE User Authentication (XUA) Architecture

XUA provides an extension to Safeguard to authenticate users based on pre-set rules that are applied on top of NonStop security settings.

Users can now access NonStop servers through an industry SSO solution. The Authentication layer will map the user to the associated NonStop userid.

Configuration Settings and Authentication Rules

USERID Information

SAFEGUARD

NonStop Programs - TACL, OSS, FTP, ODBC, DSM/SCM, SSH, OSM and all others

User Authentication

Safeguard consults XUA on authentication requests.

Audit Data
(Audits can be captured in up to 9 locations simultaneously)

User activities can be monitored and audited.

SEEP Evaluation

- XYGATE XUA is a Safeguard authentication Security Event Exit process (SEEP)
- SEEPs are configured using SAFECOM (or SPI)
- SEEPs are exits where Safeguard will check to see if an external product is defined and active, and if so, will pass a request evaluation message to the product before evaluating the request under Safeguard's own rules.
  - If the SEEP returns NO, the request is denied
  - If the SEEP returns YES, Safeguard then evaluates the request itself and abides by the decision made based on Safeguard's rules

Logon Controls

- Safeguard:
  - Userid or alias
  - 64-character password or pass-phrase
  - Basic password quality options
  - Global setting of maximum bad attempts
  - Global setting of either fail-freeze or timeout when maximum bad attempts is reached
- XYGATE UA extensions:
  - Individual settings of maximum bad attempts
  - Individual choice of fail-freeze, timeout, or process-stop when maximum bad attempts is reached

Sample XUA Rules – developers (1)

```
UAGROUP Developers-From-Work
  DESCRIPTION "Developers from local internet"
  FROM_USER 0,0
  TO_USER $DEVELOPERS
  AUTHENTICATE_MAXIMUM_ATTEMPTS 5
  AUTHENTICATE_FAIL_STOP ON
  PORT 10.1.1.*
```

XYGATE User Authentication ACL Group

Sample XUA Rules – Developers (2)

```
UAGROUP Developers-From-Home
  DESCRIPTION "Developers from non-local internet"
  FROM_USER 0,0
  TO_USER $DEVELOPERS
  REQUESTOR $SEC.XYGATEAC.XYGATEAC
  AUTHENTICATE_MAXIMUM_ATTEMPTS 5
  AUTHENTICATE_FAIL_FREEZE ON
  PORT +.+.+.+
```

Sample XUA rules – developers (3)

```
UAGROUP Developers-From-Bad Location
  DESCRIPTION "Developers from non-local internet without XAC"
  FROM_USER 0,0
  TO_USER $DEVELOPERS
  PORT +.+.+.+
  RESULT_DENIED
```

XUA Testing Rules and Extensions

- XUA has an explain capability that allows you to specify the operation
- XUA then explains how it chooses the appropriate rule group
- The WHAT-IF testing tool
  - Can use production or alternate security rule set
  - Replicates logic for decision making to allow rule testing or "why did it do it this way" research
  - Provides a method for repeatable testing

XYGATE Access Control – future offering!

Product Features

XYGATE Access Control, available in the future from HP, provides security capabilities that allow customers to set granular controls on the access to all resources of the system.

- Eliminates shared UserID use – all user tasks can be performed from a single user.
- Allows customer to control who can perform commands and sub-commands within NonStop utilities.
- Provides complete key stroke logging to monitor user activities and achieve accountability.
- Will be available as an independent product shipped on a CD for J Series, H Series and G Series.

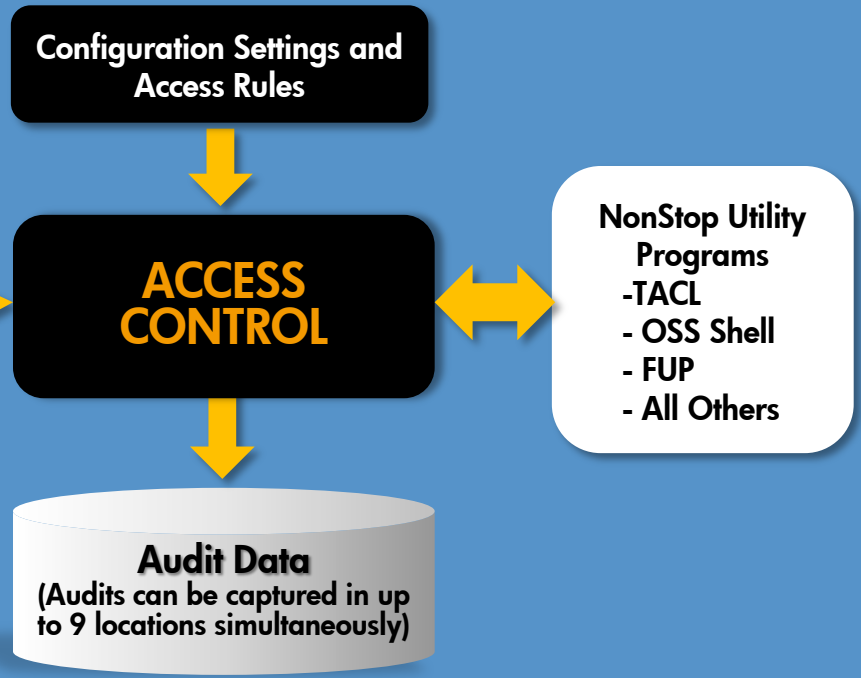
XYGATE Access Control (XAC) Architecture

Access controls are configured on the system

As users attempt to access system resources, the Access Control layer checks their rights and allows or denies access accordingly

User activities are monitored and audited, to the keystroke level if desired.

PC/Terminal



XYGATE Access Control – Shared IDs

- Each user only requires one ID
  - Can be a Guardian User or Alias
  - No need for Super group level (255,*)
  - No need for Manager user level (*,255)
- Can grant privileges based on need
- Passwords to sensitive IDs are not required

XYGATE Access Control – Shared IDs

- Example – SUPER.SUPER Access to SCF via Guardian

```
$VDBF BARRY 4> logon super.super
Password: ********

Welcome to the XYPRO Technology Production Computing Facility \XYS7000.

Last Logon:  12 APR 2010, 22:17
Last Unsuccessful Attempt: 12 APR 2010, 22:11  Total Failures: 3361
$SYSTEM SYSTEM 5> scf
SCF - T9082G02 - (06JAN06) (31OCT05) - 04/13/2010 06:57:11 System
\XYS7000
(C) 1986 Tandem (C) 2006 Hewlett Packard Development Company, L.P.
(Invoking \XYS7000.$SYSTEM.SYSTEM.SCFCSTM)
1->
```

SCF Running as SUPER.SUPER

- All product views are illustrations and might not represent actual product screens

XYGATE Access Control – Shared IDs

- Example – SUPER.SUPER Access to SCF via XYGATE Access Control

```
$VDBF BARRY 5> xac scf-255

XAC - \XYS7000.XYPRO.BARRY Password: ********
XYGATEAC 5.52 XYPRO Eastern North America \XYS7000 20110630 (see
>CONFIG for Copyright)
SCF - T9082G02 - (06JAN06) (31OCT05) - 04/13/2010 07:06:19 System
\XYS7000
(C) 1986 Tandem (C) 2006 Hewlett Packard Development Company, L.P.
(Invoking \XYS7000.$SYSTEM.SYSTEM.SCFCSTM)
1->
```

SCF Running as SUPER.SUPER

- All product views are illustrations and might not represent actual product screens

XYGATE Access Control – Shared IDs

- Example – SUPER.SUPER Access to SCF via XYGATE Access Control – Basic Configuration

```
COMMAND SCF-255                      ! Command executes SCF as SUPER.SUPER
    DESCRIPTION                      "SCF as SUPER.SUPER"
    USER 255,255                     !Executes as SUPER.SUPER
    OBJECT $SYSTEM.SYSTEM.SCF        !Executes SCF
    ACL $SUPER                       !Only privileged users can execute this
    VERIFYUSER $EVERYONE             !Validate user executing the command
    TIMEOUT 900                      !Stop after 15 minutes of inactivity
    PASSWORDTIMEOUT 600              !Ask for password again after 10
                                     !minutes of inactivity
```

- All product views are illustrations and might not represent actual product screens

XYGATE Access Control – Role Based

- XYGATE Access Control ACL Groups
  - –Provides Role-Based Access Control
  - –Allows for ease of administration

```
ACLGROUP $EVERYONE      \*.*.*
                        ALIAS:"\*.*"

ACLGROUP $SUPER         255,255
                        \*.222,11
                        \*.XYPRO.BARRY
                        ALIAS:"\*.barry"
                        NETUNDERLYING:222,11
```

- All product views are illustrations and might not represent actual product screens

XYGATE Access Control - Audit

- Auditing User and Alias activity is as flexible as you want it to be
  - Keystroke Audit, input and output, all activity for every user.
  - Keystroke Audit only the activity of specific users or functions.
  - Audit the commands entered from OBEY files.

XYGATE Access Control

- Auditing all user activity – Transparency

```
TELSERV Detailed Info SERVICE \NODE1.$ZTC0.XACTACL

*Type..................  CONVERSATION      *Subtype..............
DYNAMIC
*Display...............  ON                *Autodelete.............  OFF
*Owner.................  N/A               *Access.................  ALL
*CPU...................  N/A               *Pri....................  N/A
*Swap..................  N/A
*Program...............  $SYSTEM.XYGATEAC.XYGATEAC
*Lib...................  N/A
*Resilient.............  OFF
*Param.................  audited-tcpip-tacl
*Assigned Window.......  OFF
*Default Service.......  OFF
```

- All product views are illustrations and might not represent actual product screens

SAFEGUARD AND OSS SECURITY ENHANCEMENTS

Safeguard Enhancements

Recent Focus areas

- Password strength and quality
- Additional forensic information
- Improved audit granularity (especially OSS)
- Manageability improvements
- OSS controls

H06.22/J06.11 (February 2011)

- Ability to restrict OSS (POSIX) fileset access by the super ID
- Additional password quality options
- Program file ACL inheritance
- Elimination of extraneous TACL read audit for logoffs where the user does not have read access to TACL

Safeguard Enhancements: RestrictedAccess Filesets

H06.22/J06.11 (February 2011)

- A RestrictedAccess fileset is an OSS fileset in which the super-user is denied special access privileges.
  - The super-user is required to follow the fileset's file and directory permissions (standard UNIX permissions and OSS ACLs).
- A new RestrictedAccess fileset attribute has been added to OSS filesets.
- Restricted access is not the default, and must be explicitly enabled on a fileset basis.
- This feature is only supported on Version 3 filesets.
- For additional details, attend next week's update talk on Open System Services and the NonStop OS

Safeguard Enhancements: Program File ACL Inheritance

H06.22/J06.11 (February 2011)

- When a process is created, existence of NAMED/UNAMED process ACLs, as well as the existence of an ACL for the specific process name (if any) are first checked.
- If none of these predefined ACLs exist, but the objectfile does have a process-ACL record, then the ACL from the process-ACL record is inherited by the new process.

Safeguard Enhancements: Password Quality

H06.22/J06.11 (February 2011)

- Password quality attributes may now be used when PASSWORD-ALGORITHM is configured as either HMAC256 or DES
- Alpha characters (either uppercase or lowercase) may now be required (PASSWORD-ALPHA-REQUIRED)
- The minimum number of characters of a particular type may be specified:
  - PASSWORD-MIN-UPPERCASE-REQ
  - PASSWORD-MIN-LOWERCASE-REQ
  - PASSWORD-MIN-NUMERIC-REQ
  - PASSWORD-MIN-SPECIALCHAR-REQ
  - PASSWORD-MIN-APLHA-REQ

Safeguard Enhancements

H06.21/J06.10

- Reflect changes to user's security attributes immediately for all processes running with the particular user's id without having to restart the processes.
- Make disk file pattern protection records persistent at the volume level.
- Display the requestor process's program file name in Safeguard audit reports.
- Include the program file name in the audit record when a Guardian process is created.

Safeguard Enhancements: User Security Attributes

H06.21/J06.10

- Safeguard now can immediately reflect changes to the following user attributes for each process running with the particular user's id, without having to restart the process:
  - AUDIT-USER-ACTION-PASS
  - AUDIT-USER-ACTION-FAIL
  - Primary Group Number
  - Group list
  - Group count
- The new Safeguard DYNAMIC-PROC-UPDATE attribute enables or disables this feature.
  - By default, this feature is disabled.

Safeguard Enhancements: Diskfile Pattern Persistence

H06.21/J06.10

- A Diskfile-Pattern is a fully qualified filename with wild card characters in the subvolume name and/or diskfile name.

  Examples: $DATA.SUBVOL.*, $DATA.*.*

- Adding a Diskfile-Pattern creates distinct Diskfile-Patterns for each volume whose volume name matches the wild card pattern.

  Example: > SAFECOM ADD DISKFILE-PATTERN $DATA*.SUBV*.FILE*

- Prior to this release, if a new volume called $DATA02 is added later, it does not inherit the protection rules defined by this Diskfile-Pattern even though the volume name matches the pattern in the earlier ADD command.

Safeguard Enhancements: Diskfile Pattern Persistence

H06.21/J06.10

- Safeguard now stores the Diskfile-Pattern records in the SPTGUARD file, allowing them to be applied later to newly added volumes matching the pattern.
- A new Objecttype, SAVED-DISKFILE-PATTERN, is used to store the Saved-Diskfile-Pattern protection records, including the volume name with or without wildcard, as specified in the pattern.
- Safeguard creates the SPTGUARD file in the $SYSTEM.SAFE subvolume when Saved-Diskfile-Pattern protection is added for the first time.
- To create a SAVED-DISKFILE-PATTERN record:

  > SAFECOM ADD SAVED-DISKFILE-PATTERN $DATA*.SV*.FILE*, ACCESS TEST.USER1 (R, W)

Safeguard Enhancements: Diskfile Pattern Persistence

H06.21/J06.10

- After a new volume has been added, any applicable Saved-Diskfile-Pattern protection records must be explicitly applied to it using the SYNC command:

  > SAFECOM SYNC VOLUME <volume>

- This command instructs Safeguard to:
  - Retrieve all Saved-Diskfile-Pattern protection records applicable to the specified volume from $SYSTEM.SAFE.SPTGUARD.
  - Create the corresponding Diskfile-Pattern protection record entry in the $<volume>.SAFE.PATGUARD file in that volume for each Saved-Diskfile-Pattern protection record retrieved.
- Saved-Diskfile-Pattern protection records can be added, altered, deleted, frozen, or thawed.

Safeguard Enhancements: New Audit Field (1)

H06.21/J06.10

The primary audit record for all audit events contains a new field, SubjectProgramName, the program file name of the subject process (requestor process).

```
Auditnumber          =FFFE02F1AD9B181FD917
TimeReported         =2010/05/25 15:48:19     TimeReceived          =2010/05/25 15:48:19
Operation            =Start                   Outcome               =Passed   …
SubjectUserNumber    =255,255                 SubjectSystemName     =\YOSAFE
SubjectCreatorName   =SUPER.SUPER             SubjectCreatorNumber  =255,255
SubjectProcessName   =\YOSAFE.$Z11K.0,236     SubjectAuthlocName    =\YOSAFE
SubjectTerminalName  =\YOSAFE.$ZTN0.#PTLAP1Q  SubjectAuthlocNumber  =86
SubjectProgramName   =\YOSAFE.$SYSTEM.SYSTEM.TACL
CreatorUserName      =SUPER.SUPER
```

Safeguard Enhancements: New Audit Field (2)

H06.21/J06.10

- When a new Guardian process is started, the audit generated now displays the program file name of the process as part of the secondary audit record.
- The object file name is displayed as the field ObjectProgramName.
- Note that audit already included the program file name for OSS processes prior to this enhancement.

Safeguard Enhancements

G series (G06.32.01)

Selected content from H-series RVUs:

- Configurable OSS audit exclusion (H06.15)
- Creator ID and creation timestamp in user/alias/group authentication records (H06.15)
- PASSWORD program enhancements (H06.16)
- 255-byte description fields for some types of object authorization records (H06.16)
- Support for additional POSIX APIs: initgroups(), setgroups(), seteuid(), and setegid() (H06.18)
- SEEP interface enhancements for security partners (H06.18)
- $ZSMP (OSMP) released with HIGHPIN set (H06.18)
- Support PRIV LOGON using Licensed flag as a surrogate when Safeguard is down (H06.19)
- Ability to audit TACL LOGOFFs with less additional audit generated (H06.19)

Safeguard/Standard Security/OSS Security

RFEs under consideration (partial list)

- Make it possible to deny SUPER.SUPER the ability to alter user attributes such as password and default security.
- For unnamed processes, include the CPU and PIN in Authorization SEEP interface STOP requests.
- Introduce an administrative group that can be used by auditors to view/collect Safeguard information without also giving them the ability to alter the configuration.
- Provide a SEEP-style interface for OSS authorization.
- Support certificate-based authentication.
- Multithread the SMON process.

SQL/MX SECURITY ENHANCEMENTS

SQL/MX future enhancements

- Separation of duties
- Change of ownership
- Restriction of catalog/schema creation
- NSM/web firewall support
- Additional enhancements under consideration

SQL/MX separation of duties

Future release

- The problem: per the ANSI SQL 92 specification, any user who can manage object security privileges for a specified set of objects also has access to the data
- The solution: separation of duties allows designation of a class of users, the SQL/MX Security Administrators (SSA) group, who will be allowed to manage object security privileges (through GRANT/REVOKE) without being allowed to GRANT access to themselves or any other members of that class
  - If no SSAs are defined to SQL/MX, SUPER.SUPER is allowed to create the first one
  - SUPER.SUPER may be a member of the SSA group
  - If there is at least one other SSA defined and SUPER.SUPER in not included in the set, SUPER.SUPER will lose its previous authority to perform grant/revokes
- Note: to avoid circumvention, members of the SSA group should not be allowed to create new Guardian users

SQL/MX change of ownership

Future release

- Non-disruptive change of ownership without having to drop and recreate the object
- Supported for SQL/MX database objects: base tables and (implicitly) associated indexes and constraints; views; stored procedures; triggers
  - May be performed by SSAs or the object owner
  - After ownership of an object is transferred to another user:
    - The schema owner will continue to have all DDL and utility privileges on the object except for GRANT and REVOKE
    - The schema owner will not have DML privileges on the object
  - Not supported for SQL/MP objects or SQL/MP ALIAS
  - Not automatically replicated by RDF

SQL/MX change of ownership

Future release

- This is the SQL/MX analog to FUP GIVE for Guardian files
- Change of ownership for SQL/MX schemas:
  - May be performed by SSAs or the schema owner
  - Also changes ownership of associated user metadata files such as histogram tables
  - Has option to cascade the ownership change to those objects under the schema that belonged to the prior schema owner (not a single atomic transaction – run recovery tool if change fails while in progress)

- Change of ownership for SQL/MX catalogs:
  - May be performed by SSAs or the catalog owner
  - Change of ownership of a catalog does not change ownership of the underlying schemas

SQL/MX restriction of catalog/schema creation

Future release

- Limit catalog creation to a designated set of users
  - Privilege is controlled by SSAs
- Limit schema creation within a catalog to a designated set of users
  - Privilege is controlled by SSAs or the catalog owner
- Extension to GRANT/REVOKE commands

- Default remains that all users may create catalogs and schemas

Additional SQL/MX future potential security enhancements

- SSL support for ODBC/MX and JDBC/MX
- SQL statement logging
- Support for column-level encryption
- ANSI roles

ITP SECURE WEBSERVER SECURITY ENHANCEMENTS

iTP Secure WebServer Release 7.2 Enhancements

H06.21/J06.10

- Changes in supported encryption algorithms and key lengths
  - Support added for TLS 1.0 and TLS 1.1
  - Support dropped for SSL 2.0 and PCT 1.0
  - Check the documentation for details
- PUT and TRACE methods disabled by default
- Support added for UNICODE security certificates containing non-English characters in ‘Distinguished Name’

Key Lengths and Key Databases

- Release 7.2 does not support key lengths less than 1024 bits.
- The supported key length range is 1024 bits to 4096 bits.
- Key databases generated using older versions of keyadmin are not usable with the new keyadmin and vice versa.
- Release 7.2 includes a migration utility called ‘dbmigrate’ which can be used to migrate the old key database to new database.

iTP Secure WebServer potential enhancements

- Diffie-Hellman key exchange support
- Rebase to latest version of GnuTLS
- Improved tracing

In Conclusion

- Keeping your environment secure is an ongoing process
- Security products are only a part of the picture

  … but they are an important part, and HP continues to enhance the security capabilities of existing products and add new functionality to assist you in implementing a robust security management policy
- We welcome your feedback on security product requirements
  - Enhancements to existing products
  - New products

QUESTIONS?

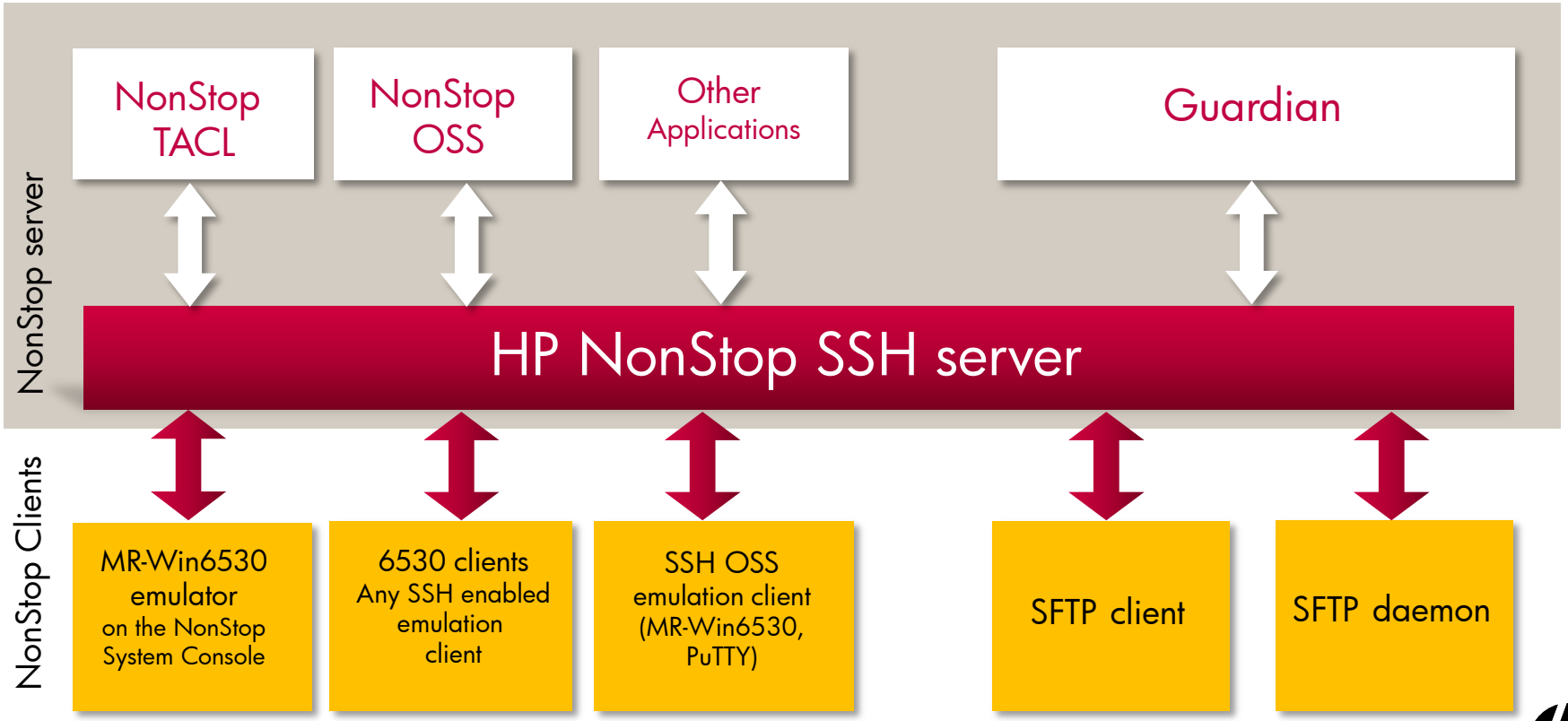
NONSTOP SECURITY CONTACTS
WHO TO CALL AT HP

Karen Copeland
NonStop Product Manager for Security
karen.copeland@hp.com

Wendy Bartlett
Distinguished Technologist, NonStop
wendy.bartlett@hp.com

MORE ON SSH AND SSL

NonStop SSH Architecture



What is the Secure Socket Layer (SSL) protocol?

- SSL (Secure Socket Layer) is a cryptographic protocol that provides security for communicating over the Internet.
  - SSL encrypts the segments of network connections at the transport layer end-to-end.
  - SSL is in widespread use for web browsing, email, instant messaging and other applications.
- Previously, NonStop customers had to purchase SSL solutions from NonStop security partners.
  - This year, HP is introducing the HP NonStop SSL product based on the SecurCS product from comForte for use on J Series and H Series servers.
  - This product provides native SSL and is included with the NonStop Operating System as another option for customers to use to secure their data in motion.

Data in Motion - SSL

Product Features

- On the NonStop platform, HP NonStop SSL is designed to run in native mode under the Guardian filesystem, resulting in optimal performance and full leverage of the NonStop advantages
  - Supports SSL for Telnet, Middleware, Expand and SFTP
  - On the client platform, there is a rich set of choices: If you have an SSL-enabled solution on the platform (such as MR-WIN6530 or MQ version 5.3) there is nothing to install
  - Will encrypt any protocol which is based on TCP clients connecting to a fixed number of static ports.
    - The TCP/IP client may reside either on the remote platform (such as for Telnet, RSC or ODBC) or on the NonStop platform (such as for FTP or FASTPTCP)

Data in Motion - SSL

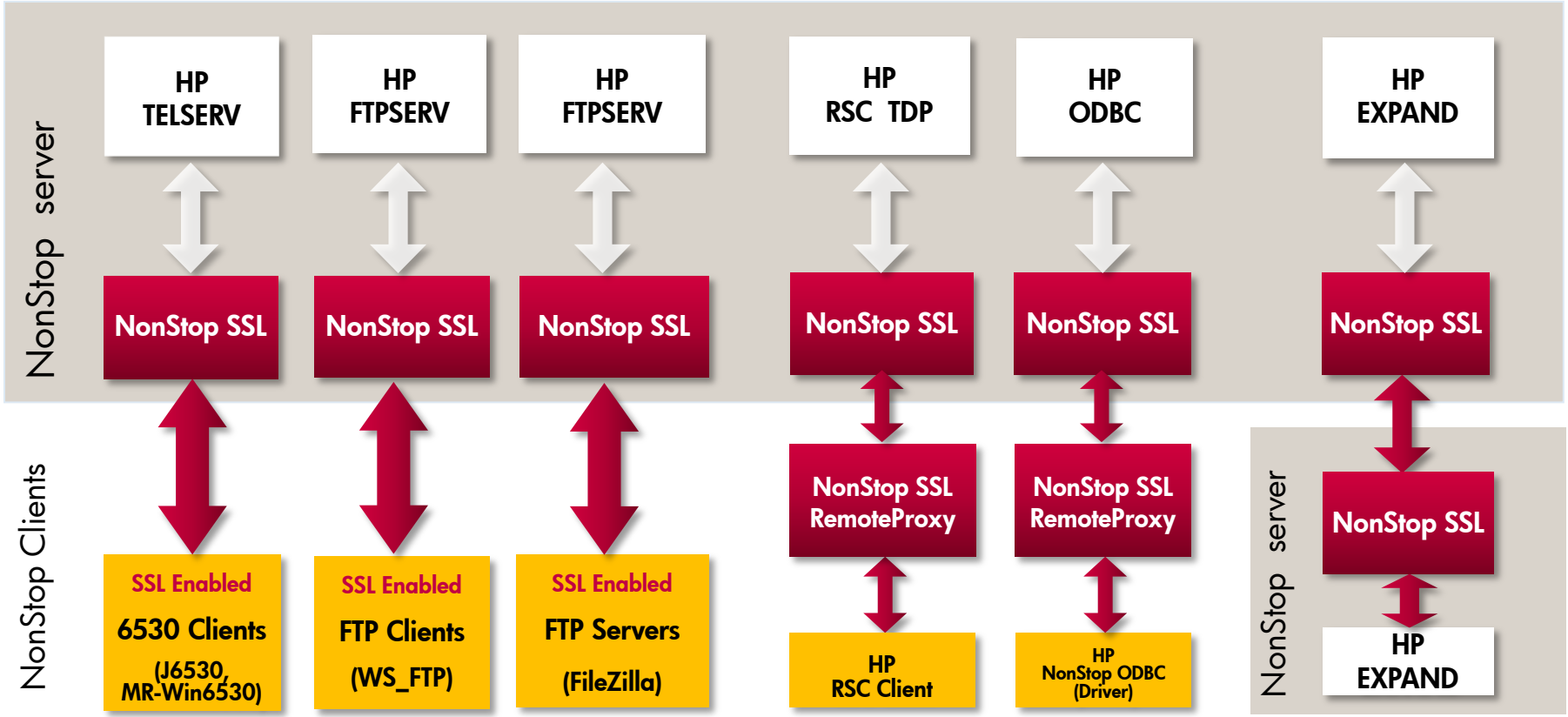
Product Features (continued)

- HP NonStop SSL can be started in different run modes to enable SSL encryption for a variety of applications and services.
- Multiple NonStop SSL processes can co-exist on a single NonStop system to support concurrent (secure and non-secure) web and proxy services, as well as multiple TCP/IP processes.
- HP NonStop SSL processes do not run as process pairs, but fault tolerance can by achieved by starting SSL processes on multiple TCP/IP stacks running in different processors.

Data in Motion - SSL

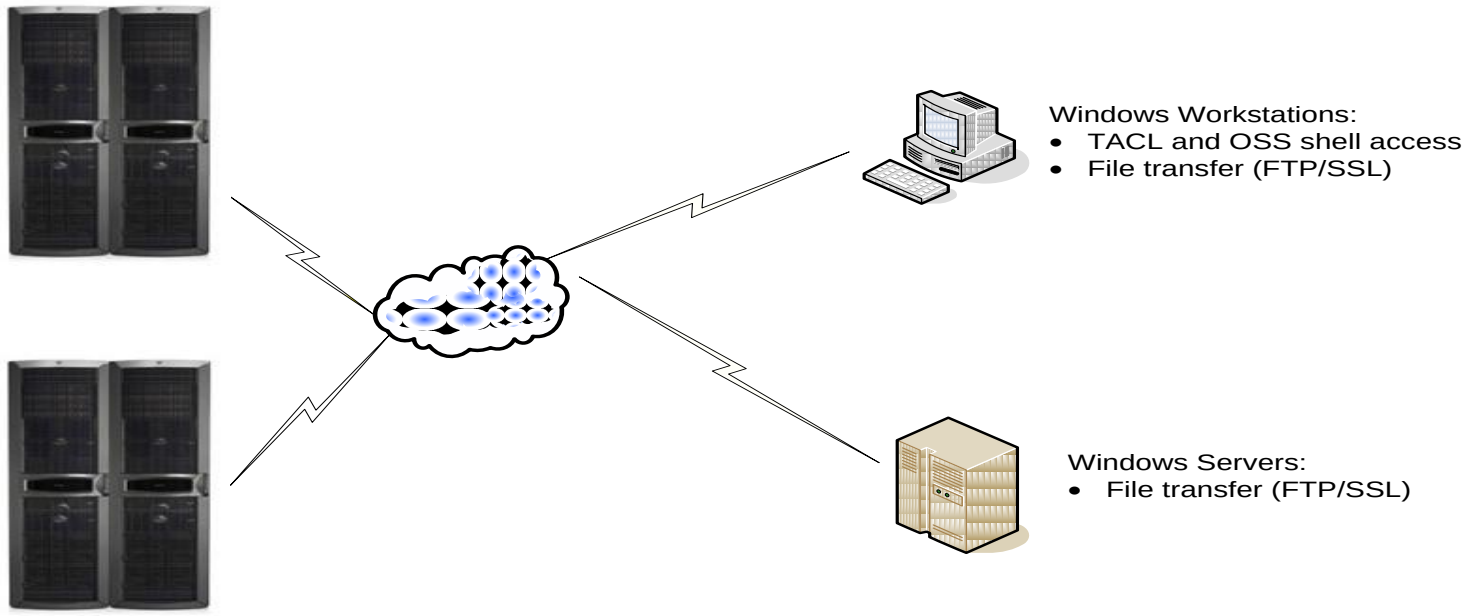
- Runs in native mode under the Guardian filesystem, resulting in optimal performance.
- Supports SSL for Telnet, Expand, Middleware and FTP
- Supports many clients: When using an SSL-enabled solution on the partner platform (like MR-WIN6530 or WS_FTP) there is nothing to install
- Can be started in different run modes to enable SSL encryption for a variety of applications and services.
- Encrypts any protocol based on TCP clients connecting to a fixed number of static ports.
  - The TCP/IP client may reside either on the remote platform for Telnet or RSC or on the NonStop platform (such as for FTP or FASTPTCP)
- Multiple NonStop SSL processes co-exist on a single NonStop system to support concurrent proxy services, as well as multiple TCP/IP processes.
- Although HP NonStop SSL processes do not run as process pairs, fault tolerance can by achieved by starting SSL processes on multiple TCP/IP stacks running in different processors.

NonStop SSL Architecture



Data in Motion – SSL

Typical Customer Usage



When SSL is "added" to a non-secure protocol an "S" is typically added to the end of the protocol name; for instance, HTTPS or FTPS

Data in Motion – SSL

Considerations for FTP/SSL

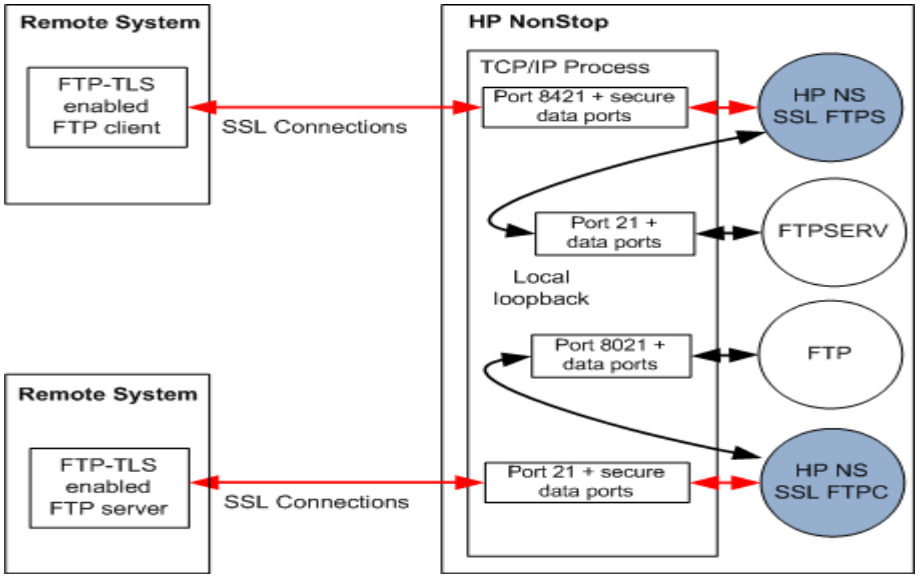
- Terminology:
  - FTP: the old and common method, not encrypted
  - FTP/SSL: works “on top of” FTP, uses SSL encryption

- FTP to FTP/SSL migration considerations
  - Rich choice of clients and servers (commercial and free) for Windows
  - Solutions for Unix available, but typically not pre-installed
  - When using a GUI client: little changes
  - Command-line syntax is identical

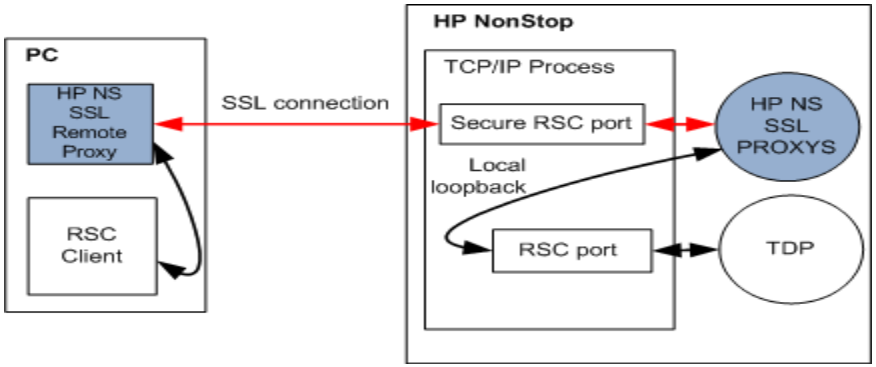
NonStop SSL Proxy Run Modes

FTPC	FTP client proxy
FTPS	FTP server proxy
PROXYC	Generic SSL client proxy
PROXYS	Generic SSL server proxy
TELNETS	Secure Telnet proxy
EXPANDS	Secure EXPAND proxy
ODBCMXS	Secure ODBC proxy

Secure FTP Proxy

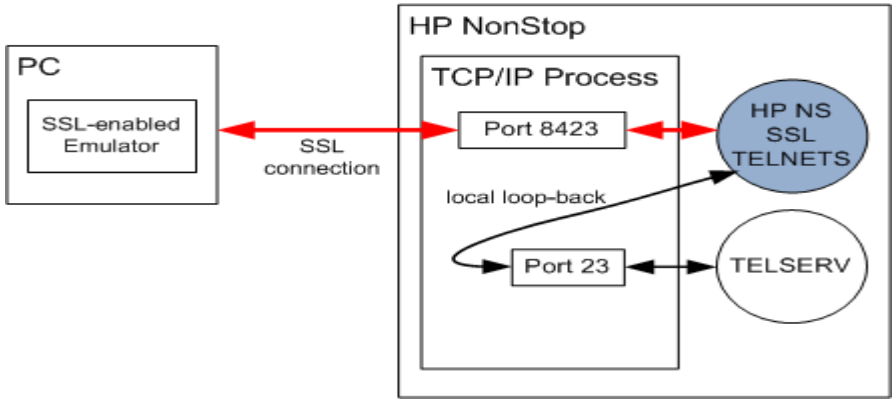


Generic TCP/IP Client/Server Protocols
Example: RSC

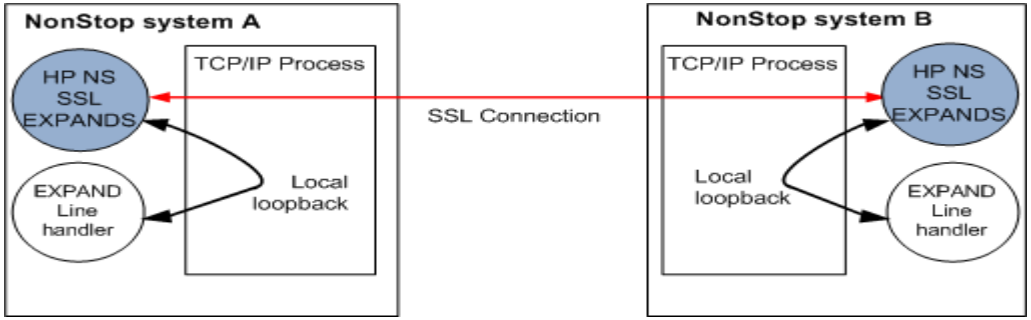


ODBC/MP fits into this model

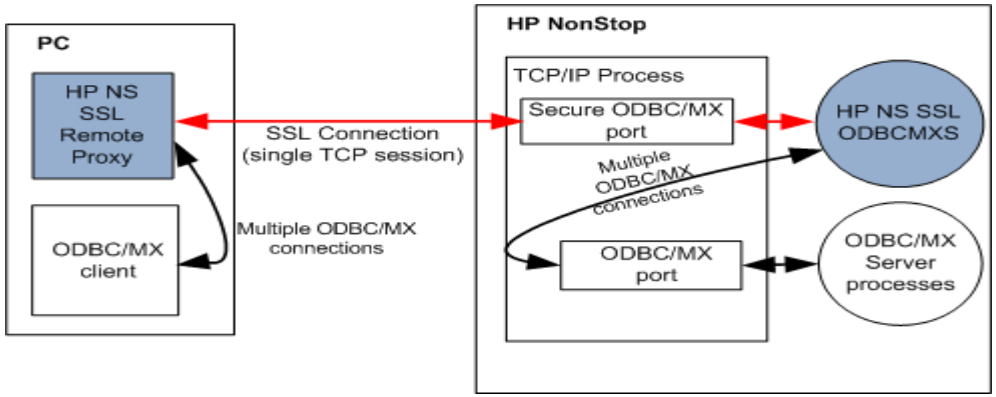
Secure Proxy for Telnet Access



Secure Proxy for Expand over IP



Secure Proxy for ODBC Drivers



Multiple ODBC/MX sessions are tunneled over a single TCP session

Limiting Remote IP Addresses

- HP NonStop SSL can be configured to allow only certain remote IP addresses. By default, HP NonStop SSL will allow connections from any IP address; this behavior can be changed by:
  - Setting a "black list" of forbidden IP addresses using the DENYIP parameter.
  - Setting a "white list" of allowed IP addresses using the ALLOWIP parameter.

- Note: the black list will take precedence over the white list: if an IP address is matching both lists, it will NOT be allowed.

Comparison between SSH and SSL

Topic	SSH	SSL
Origin	UNIX/Linux environments	Windows and mainframe environments
Cryptography Method	Uses Public/Private key cryptography	Uses Public/Private key cryptography
Encryption algorithm	Uses symmetric encryption algorithm	Uses symmetric encryption algorithm
Method	Requires each endpoint to individually trust every other endpoint using a public key or user name and password or password authentication	Uses “certificate authority” method or “CA” to delegate trust by issuing certificates for authentication.
Telserv Approach	Completely replaces Telserv layer on the system	Uses a proxy-based approach to address Telserv
Advantages	Easier self key generation and configuration.	Easier large scale deployment for HTTP over SSL (HTTPS)

When to use SSL vs. SSH

Protocol to secure	Method	Notes
Telnet	SSL, SSH	Usage may depend on customer's: -Emulator capabilities -Corporate Policy -Legacy Environment Industry Trend is to use SSH
File Transfer	SSL, SSH (SFTP)	Usage may depend on customer's: -Partner Systems (SFTP very popular on UNIX) -Corporate Policy -Legacy environment Industry trend is to use SSH (SFTP)
EXPAND	SSL	SSH not supported with EXPAND
ODBC	SSL, (SSH)	SSH only possible with port forwarding, which may be very complex to setup for ODBC
RSC	SSL, (SSH)	SSH only possible with port forwarding. SSL is more straight-forward.

MORE ON XUA

Sample XUA rules – to SUPER.SUPER

```
UAGROUP SUPER-SUPER-Limits-2
  DESCRIPTION "SUPER.SUPER rule #2"
  FROM_USER $EVERYONE
  TO_USER SUPER.SUPER
  REQUESTOR $SEC.XYGATEAC.XYGATEAC
  AUTHENTICATE_MAXIMUM_ATTEMPTS 3
  AUTHENTICATE_FAIL_TIMEOUT 60
```

Sample XUA rules – from SUPER.SUPER

```
UAGROUP SUPER-SUPER-to-other-users
 DESCRIPTION "SUPER.SUPER rule #3"
  FROM_USER SUPER.SUPER
  TO_USER $EVERYONE
  AUTHENTICATE_MAXIMUM_ATTEMPTS 3
  AUTHENTICATE_FAIL_TIMEOUT 60
  FROZEN_OK ON
  REQUESTOR $SEC.XYGATEAC.XYGATEAC
```

Sample XUA rules – unapproved userids

```
UAGROUP Prohibit-all-not-approved
  DESCRIPTION "Final screen of all unapproved userids"
  FROM_USER $EVERYONE
  TO_USER $EVERYONE
  REQUESTOR $*.*.*
  ANCESTOR $*.*.*
  AUTHENTICATE_MAXIMUM_ATTEMPTS 3
  AUTHENTICATE_FAIL_TIMEOUT 60
  RESULT_DENIED
```

MORE ON SAFEGUARD

Safeguard Enhancements

H06.20/J06.09 (February 2010)

- Adds support for NFS OSS Access Control Lists (ACLs)
- Have FUP display the “Safeguard-protected” **** security string for diskfiles placed under Safeguard control using DEFAULT-PROTECTION or PERSISTENT PROTECTION records
- Adds a LOGON program option for self-stop after authentication

Safeguard Enhancements

Released in 2009

- H06.19/J06.08 (Sept 2009)
  - Support PRIV LOGON using Licensed flag as a surrogate when Safeguard is down
  - Add a "MID" search option to CHECK-DISKFILE-PATTERN attribute to provide more flexibility
  - Ability to audit TACL LOGOFFs with less additional audit generated
  - Additional audit information:
    - Actual file system error for failure cases
- H06.18/J06.07 (May 2009)
  - Support for additional POSIX APIs: initgroups(), setgroups(), seteuid(), and setegid()
  - SEEP interface enhancements for security partners:
    - Inclusion of object file name in Authorization SEEP structure
    - Evaluation of password change request before sending the password event to a Password Quality SEEP
  - Wild card support for GROUP ADD MEMBER and ALTER MEMBER commands
  - $ZSMP (OSMP) released with HIGHPIN set

MORE ON ITP SECURE WEBSERVER

Encryption Algorithms in Release 7.2

- Support for AES and Camellia ciphers has been added.
- Support for RC2, DES and ARC4-40 encryption algorithms has been discontinued as they are considered insecure.
- The encryption algorithms supported with SSL 3.0 and TLS are:

Encryption Algorithm	Supported with SSL 3.0	Supported with TLS
AES-256-CBC	Yes	Yes
AES-128-CBC	Yes	Yes
3DES-CBC	Yes	Yes
ARC4-128	Yes	Yes
CAMELLIA-256-CBC	No	Yes
CAMELLIA-128-CBC	No	Yes

Message Authentication Code (MAC) algorithms

- For TLS, iTP Secure WebServer uses hashed MAC algorithms instead of simple MACs for increased security.
- It continues to use the simple MAC algorithm in SSL 3.0 sessions.
- The following MAC algorithms are supported with both TLS and SSL:
  - SHA1
  - MD5

Disabling PUT and TRACE HTTP methods by default

- Because of the security vulnerabilities introduced by these methods, iTP Secure WebServer now disables PUT and TRACE methods by default.
  - The PUT method allows a client to upload arbitrary web pages on the server.
  - The TRACE method allows the client to see what is being received at the other end of the request chain and use that data for testing or diagnostic information.
- Prior versions of iTP Secure WebServer enable both methods by default.
  - If you are running one of these versions, we strongly recommend disabling both methods.
- User must explicitly configure the PUT method when configuring under 'Region' command. The default value will be Off.
- The syntax for configuring the TRACE method is as follows:

HTTPTraceMethodEnable <On/Off>

FORWARD-LOOKING STATEMENTS

This document contains forward looking statements regarding future operations, product development, product capabilities and availability dates. This information is subject to substantial uncertainties and is subject to change at any time without prior notification. Statements contained in this document concerning these matters only reflect Hewlett Packard's predictions and / or expectations as of the date of this document and actual results and future plans of Hewlett-Packard may differ significantly as a result of, among other things, changes in product strategy resulting from technological, internal corporate, market and other changes. This is not a commitment to deliver any material, code or functionality and should not be relied upon in making purchasing decisions.