SSL 5.1.5.3
Released on February 1, 2006

Fixes

Re-signed Java applets.
  The Java applets have been re-signed with certificates that are valid until January, 2008. (CR Q01281857)

Fixed SSO setting for SiteMinder authentication.
  A /cfg/vpn #/aaa/auth #/siteminder/sso setting of "true" could revert to the default value of "false" when the system was rebooted.

Fixed CLI wizards.
  The changed handling of port numbers in service definitions introduced in 5.1.5.2 caused the /cfg/quick and /cfg/vpn #/aaa/quick wizards to fail (port was set before protocol). (CR Q01295758)

Fixed problem with Citrix applet using regedit, requiring admin rights.
  Citrix Java Applet uses old regedit proxy extraction method that requires administrator rights. Now the applet uses the getproxy utility the same way as the regular portforwarder applet. (CR Q01285170)

Fixed SSL proxy crash.
  Some combinations of HTTP and HTTPS requests done through the HTTP proxy applet could cause the SSL proxy to crash (and restart).

Fixed reverse rewrite problem of urls.
  Different urls are tagged with a type when they are rewritten by the NVG, eg. a javascript src url myscript.js is tagged like myscript.js,xct1
  The ,xct1 was not removed when doing reverse rewrite, this has been corrected.

Reverted fix for Japanese directory and file deletion error.
  The hex encoding used in 5.1.5.2 to work around the problem with Internet Explorer (CR Q01195775) had several negative side effects for smb/ftp access (portal links did not work, hex-encoded file names were used by browser when downloading). The fix has now been reverted until a better solution can be found.

Raised limits on X-SSL header.
  The Subject and Issuer information, included in the X-SSL header when /cfg/ssl/server #/http/sslheader is set to "on", was limited to max 255 characters each (truncated if longer). This limit is now raised to 1000 characters. (CR Q01290075)

Improved Radius Accounting for VPN users.
  The Radius Accounting information now includes the Calling-Station-Id (client IP address) attribute, and in the case of NetDirect or IPsec sessions, also the Framed-IP-Address (assigned IP address) attribute. (CR Q01216792)

Fixed link in portal Full Access tab.
  The link to www.java.com in the Full Access tab did not work, due to incorrect quoting. (CR Q01274927)

Fixed PKI authentication loop with TunnelGuard.
  If certificate authentication was used in combination with

TunnelGuard, and the TG tests failed, the user was redirected to the login page, which would automatically cause a new cert login attempt immediately. The user will now be redirected to the auto login page in case of TG failure and certificate login - this page will show the TG failure reason (just like the normal login page). (CR Q01264690)

Fixed problem starting applets from multiple portals.
When starting applets from more then one portal in the same browser session, applets from the second portal would stay pending with the message "Applet is initializing please wait". (CR Q01288347)

Enhanced tab completion for the /cfg/vpn/aaa/network/subnet CLI command.
Depending on how the subnet is configured either the name or a combination of host/mask is used. (CR Q01173628)

Enhanced tab completion for the /cfg/vpn/linkset/link CLI command.
The configurable link text is used for tab completion.
If the link text is longer than 11 characters the first 8 chars is used postfixed with "...". (CR Q01123899)

Fixed the display of password expiry alert for LDAP user:
Password expiry information will be displayed at login to the portal, only when 5 days(or less) remains before the password expires.
But sometimes when used with IE Cache Wiper, the password expiry alert seems to be blocked by the Cache Wiper.

Fixed the import of wrong file size of sdconf.rec for RSA.
Check for the sdconf.rec file size has been added. From the RSA Knowledgebase, the sdconf.rec file should always be 1024 bytes in all instances of ACE/Server 5.x and ACE/Agent 5.x.
If in future RSA ACE Releases, the sdconf.rec file size changes, then this fix should be revisited.

Fixed the SMB and FTP upload of filenames with special characters.
SMB and FTP upload with file names with special character like (@#$%foo.txt) is fixed. (CR Q01161886)

Fixed problem when sending client certificates to portal server.
When having /cfg/vpn #/server/http/addclicert set to "on" and using certificate authentication, the authentication could fail in some cases. In particular this has been observed with some certificates issued by an intermediary CA in combination with a secondary authentication method. (Found in verification of CR Q01255568)

==========
SSL 5.1.5.2
Released on December 15, 2005
==========

Fixes

Fixed buffer overflow in BBI code.
Sending an extremely long username when attempting login to the admin BBI would cause a crash in the backend server due to a buffer overflow. In principle the buffer overflow could also be exploited to give interactive OS access without authentication if the username contents was carefully crafted. (CR Q01256093)

Fixed memory leak when using HTTP compression.
Enabling compression of http data (/cfg/ssl/server #/http/compress on) caused memory leaks on sessions where compression was done, which could eventually lead to a restart of the SSL proxy (error message

"internal error 179"). (CR Q01242859)

Fixed SSL proxy restart after 497 days of uptime.
If the system had been running for 497 days without reboot, the SSL proxy would restart due to an inconsistent return value from a kernel timer function. Also the reported uptime from /info/local would start over at 0 after 497 days. (CR Q01249382)

Fixed Port Forwarder fails if certificate in the CaChain has not set Path Length Constraint.
If a certificate in the CaChain had not set the Path Length Constraint value a Port Forwarder would fail, when setting up the tunnel. (CR Q01262835)

Fixed Sub-CA Certificates authentication and authorization
Configuring the SubCA alone in the CA chain doesn't allow the user to get authenticated and authorized.(CR Q01154557)

Fixed ICMP service configuration lists port
Configuring ICMP service displays port number which is unnecessary.
/cfg/vpn #/aaa/service #/icmp
(CR Q01163667)

Fixed Japanese directory and file deletion error.
Deleting directories and files with Japanese names from smb and ftp server the deletion was successful but error messages are displayed. Internet explorer destroys the Japenese file and directory names which is prevented by special encoding schemes. (CR Q01195775)

Fixed an internal AAA subsystem restart.
The system allows the AAA subsystem to restart due to eventual internal SW failures.
However, a control channel to the traffic handling subsystem was not reinitialized properly which much later could lead to a new AAA subsystem restart (due to reuse of resources).
Note: the AAA restart only affects current login attempts (not already authenticated sessions), i.e. the users has to do a new login attempt.

Fixed oper CLI user rights.
The oper CLI user no longer has access to the following commands:
/cfg/sys/dns
/cfg/lang/import,export,vlist,del
/cfg/quick
/cfg/test
(CR Q01257387)

Fixed packets sent to client with interface IP source address.
In some cases, during the SSL-VPN logout procedure, packets could be sent to the client using the public interface IP address rather than the VIP as source address. This has only been observed on SSL-VPN when using a special test client. (CR Q01227011)

Fixed Port range backward range acceptance.
The port range backward range like 89-80 is not allowed for the following command.
/cfg/vpn #/aaa/service
(CR Q01173644)

Fixed Siteminder Agent premature timeouts and cyclic restarts.
In the event of a Policy Server becoming unreachable the AAA subsystem would restart the Siteminder Agent due to long response times. In some cases it would go into a state of continuously

restarting the Siteminder Agent before it could initialize
properly. The Siteminder Agent API has also been
upgraded (5.50.0323.860) to provide faster initialization when
Policy Servers are unavailable. (CR Q01253126)

Syslog messages added.
Added syslog message when Siteminder Agent is timed out during
initialization.
Added syslog message when Siteminder Agent is timed out during
authentication request.
Added syslog message when login time reaches a quarter of Siteminder
timeout value.

Fixed problem with MAC adress getting changed.
In some cases, e.g. when adding port 3 to an existing interface on NVG
3050, the "host" MAC address as given by /info/local would get changed,
causing a mismatch with existing licenses. (CR Q01263974)

Fixed so that non ascii passwords is handled correctly.
This is when using a ntlm type of login service.

Fixed secondary authentication in combination with certificate login.
(CR Q01255568)

Fixed memory allocation bug in the MD4 code when doing NTLM
authentication.
An incorrect memory allocation could potentially cause a system
crash/restart.

Added command .../aaa/auth #/ldap/enashortgrp.
This makes it possible to extract the first part of a returned
Distinguished Name as the group name to be used. Example:
CN=My Group,CN=User,DC=company,DC=com will use 'My Group' as the
actual group name.

Fixed problem with aaa/ldap attribute parsing being case sensitive.
(It is now case insensitive.)

Added new method for finding LDAP group information suited for iPlanet.
A new CLI menu .../aaa/auth #/ldap/groupsearch has been added.

Fixed problem with apostrophe in language definition file.
Apostrophes in the language definition file were not handled
correctly. (CR Q01177838)

Fixed non-translated messages in the portal.
Error messages given on failed login to the portal were not
translated. (CR Q01177727)

==========
SSL 5.1.5
Released on November 07, 2005
==========

For release information of the SSL-5.1.5 release, please refer to
the 'Release Notes' document accompanying the SSL-5.1.3 release.
This README will describe changes in forthcoming releases.

==========
Software Installation and Upgrade Notice
==========

The software is delivered in two different forms, as described below.

- SSL-5.1.x-upgrade_complete.pkg

  Using this package is the preferred method for upgrading an existing SSL VPN cluster, as the upgrade is propagated across the cluster and all current configuration is preserved.

  The upgrade procedure is described in "Performing Minor/Major Release Upgrades" in Chapter 4 in the SSL VPN User's Guide.

- SSL-5.1.x-boot.img

  Using this image will reset the SSL VPN device to its factory default configuration. It must be used when an SSL VPN device with different software installed is to be added to a cluster, to bring the additional SSL VPN device to the same software version as in the cluster before joining it to the cluster.

  The software reinstall procedure is described in "Reinstalling the Software" in Chapter 3 in the SSL VPN User's Guide.

Disk repartitioning required for version 5.x on some systems

This applies to the following systems:

- ASA 310, ASA 310 FIPS, ASA 410, delivered with a software version prior to 4.0 pre-installed.

- AAS 2424-SSL delivered with a software version prior to 5.0 pre-installed.

On these systems, the existing disk partitioning does not allow for a 5.x version to be installed simultaneously with version 4.2 or later. I.e. it isn't possible to do a standard upgrade from 4.2 to 5.x, or from one version of 5.x to another. Upgrade from versions earlier than 4.2 to 5.x, and software reinstall using a 5.x version, is still possible. Hence the following applies regarding standard upgrade to version 5.0 for clusters that include systems of the above type:

Current version	Procedure
4.1.x or earlier	Upgrade to 5.0, and repartition before subsequent upgrade.
4.2.x before 4.2.1.11	Upgrade to 4.2.1.11 or later 4.x, repartition, and then upgrade to 5.0.
4.2.1.11 or later 4.x	Repartition before upgrade to 5.0.

When 5.x is installed, the /boot/software/download command will give an error if one or more systems of the above type are running in the cluster, listing the hosts that need disk repartitioning. To support the repartitioning procedure, the following commands are present as of version 4.2.1.11:

/boot/software/repartcheck
  - check for and report hosts in the cluster that need repartitioning.

/boot/repartition
  - initiate repartitioning for the local host.

/cfg/sys/cluster/host #/repartition (4.2)
/cfg/sys/host #/repartition (5.x)
  - initiate repartitioning for the given host (which must be running).

These commands are "hidden", i.e. not shown in the menu or considered for auto-completion via <TAB>, since they shouldn't be used in normal operation.

During the repartition, which includes two automatic reboots, the host will effectively be out of service. The time required for the repartition is approximately:

  4-5 minutes for ASA
  7-10 minutes for AAS 2424-SSL

NOTE: It is vitally important to avoid power cycle, reset, or any other manually initiated reboot of the host while the repartition procedure is running - this may lead to a totally non-functional system.

NOTE: On the AAS 2424-SSL, after repartition is completed, it will not be possible to downgrade to software versions prior to 4.2.1.8, even via software reinstall.

Upgrading from Versions Earlier than 2.0.11.15

If you are currently running a software version earlier than 2.0.11.15, upgrade to version 2.0.11.15 (or a later 2.0.11.x version) prior to upgrading to version 3.x or later. The "intermediate" upgrade to version 2.0.11.15 is necessary in order to maintain your current configuration, and to provide reliable fallback in case the upgrade should fail.

Downgrading to Versions Prior to 5.0.x

SSL VPN clusters running software version 5.x cannot be downgraded to software version 4.x or earlier and still retain the configuration. To downgrade such a cluster to a version lower than 5.x, a complete software reinstall using the boot.img must be performed, followed by manual reconfiguration of the cluster. This is due to changes in the internal database format.