nefsis
a Brother company

Web, VoIP, and video conferencing software

Nefsis® FIPS Edition

The Nefsis FIPS Edition was designed for U.S. government agencies requiring FIPS 140-2 compliant web, VoIP, and video conferencing on their own virtual conference server or private video conferencing cloud.

This is an on-premise, installable software solution that includes all client, access point, and virtual conference server software. Nefsis supports multipoint HD video using off-the-shelf peripherals for desktops and rooms.

Nefsis technologies such as firewall and proxy traversal, scalable video coding (variable bitrate), automated bandwidth throttling, and multi-core parallel processing enable video conferencing over a wide range of Internet connection types. Nefsis FIPS Edition conferencing is secure, with configuration settings limited to 140-2 compliant options.

Features

Multipoint HD Video Conferencing

Nefsis video conferencing supports unlimited multipoint video in standard definition and high definition (HD) quality. Nefsis uses off-the-shelf webcams, HD webcams, and pan-tilt-zoom conference room video cameras. The conference host can 'play all,' play each video individually, and adjust video quality within the limits of the capture device and available bandwidth on a per-connection basis.

For Desktops and Conference Rooms

Nefsis video conferencing software supports mixed desktop and room installations. Nefsis firewall and proxy traversal also permits conferencing among multiple offices and external desktop participants connecting over the public Internet.

Advanced Collaboration Tools

Nefsis includes a full-suite of advanced collaboration tools for sharing virtually anything accessible to the presenter's PC. Nefsis provides document and PowerPoint® presentation sharing; live application, region, and desktop sharing; white boarding and text chat. There is no need to preload data before a conference begins, conference hosts can share materials in real time. Advanced features include annotation over live applications, media file sharing (play a movie file during conference), electronic handouts, and audio/video/data conference recording in industry standard file formats (AVI, Flash).

Security, FIPS Compliance, and IT-Friendly Controls

Nefsis FIPS Edition video conferencing is secure, sending all web, VoIP and video data over end-to-end encrypted connections. All security certificate, authentication, communications transport (TLS), and ciphers use FIPS 140-2 compliant methods. In addition, Nefsis includes a comprehensive set of administrative tools including usage reports, user and feature controls, and built-in network diagnostics.

For a complete list of features, please refer to the Nefsis standard data sheet.

Nefsis is Compliant with the Following FIPS Standards

-FIPS 186-2 Digital Signature Standard RSA and DSA
-FIPS 180-1, 180-2 Secure Hash Standard SHA-1
-FIPS 197 Advanced Encryption Standard (AES)
-FIPS 46-3 Triple-DES
-FIPS 198a Keyed-Hash Message Authentication Code (HMAC)
-FIPS 140-2

Nefsis and Windows O/S Policy Regarding Communication Transports

When FIPS-compliant settings are enabled on the Nefsis server, it will enable the FIPS operating system policy on Windows (HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy\Enabled) and (HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy). This policy will force Nefsis to use communication transports that leverage the existing FIPS-140-2 compliant encryption in Windows 2003 or 2008 server.

For additional details, please refer to the Windows communication transport layer and how it works with FIPS-140: http://technet.microsoft.com/en-us/library/cc750357.aspx.

FIPS compliant settings only allow AES, 3DES and SHA hashes. Nefsis will only use the following protocols in FIPS-140-2 mode:

RSA_3DES_SHA	DH_RSA_3DES_SHA	DHE_RSA_3DES_SHA
RSA_AES128_SHA	DH_RSA_AES128_SHA	DHE_RSA_AES128_SHA
RSA_AES256_SHA	DH_RSA_AES256_SHA	DHE_RSA_AES256_SHA
DH_DSS_3DES_SHA	DHE_DSS_3DES_SHA	DH_ANON_3DES_SHA
DH_DSS_AES128_SHA	DHE_DSS_AES128_SHA	DH_ANON_AES128_SHA
DH_DSS_AES256_SHA	DHE_DSS_AES256_SHA	DH_ANON_AES256_SHA

Nefsis is Compliant with the Following NIST & IETF Requirements

NIST 800-52 Transport Layer Security Guidelines
IETF RFC 2246 TLS/SSL Protocol, Version 1.0
IETF RFC 3268 AES Cipher suites for TLS
IETF RFC 2104 HMAC-SHA-1

Nefsis Server System Requirements

-Intel Core2Duo 3.0GHz or better
-2GB RAM available for each Nefsis server component (APS & VCS)
-4GB hard drive space
-Windows Server 2003 SP3 or Windows Server 2008
-.NET Framework 3.5 installed with the latest updates
-2 static IP addresses (can be physical or mapped, but must be static)
-for additional information regarding ports, virtualization environments, please visit:
http://www.nefsis.com/Support-Video-Software/conferencing-server-requirements.html
-for additional information regarding client software system requirements, please visit:
http://www.nefsis.com/Support-Video-Software/conferencing-system-requirements.html

Additional Nefsis Reference Material

Please refer to the standard Nefsis data sheet for more information on conferencing features:
http://www.nefsis.com/pdf/nefsis-datasheet.pdf
Compatible video conferencing equipment:
http://www.nefsis.com/Best-Video-Conferencing-Software/video-conferencing-equipment.html
Online user guide:
http://www.nefsis.com/manual/user-manual.html
Contact Nefsis for server installation and client software deployment guides.

Nefsis FIPS Edition includes client and server software only; it does not include audio/video peripherals and bandwidth.