امکان مورد استفاده در Sophos UTM	راه حل
WebAdmin, User Portal, Mail Manager, SPX reply portal	Disable the use of SSLv3: Logon to the shell of the UTM as root Navigate to /var/chroot-httpd/etc/httpd/ Open the httpd.conf with vi: vi httpd.conf Add '–SSLv3' to the following line within the configuration file: SSLProtocol all -SSLv2 Example: SSLProtocol all -SSLv2 -SSLv3 Save your changes and close the editor: :wq Now restart the httpd daemon: /etc/init.d/httpd restart
Web Application Firewall	Disable the use of SSLv3: Logon to the shell of the UTM as root Navigate to /var/chroot-reverseproxy/usr/apache/conf/ Open the httpd.conf with vi: vi httpd.conf Add '–SSLv3' to the following line within the configuration file: SSLProtocol all -SSLv2 Example: SSLProtocol all -SSLv2 -SSLv3 Save your changes and close the editor: :wq Now restart the httpd daemon: /var/mdw/scripts/reverseproxy restart
SMTP Proxy	Disable SSLv3 for SMTP and turn TLSv1.2 back on: Navigate to /var/chroot-smtp/etc/ Open the exim.conf with vi: vi exim.conf Insert :!SSLv3 to the end of tls_require_ciphers Remove the line openssl_options = +no_tlsv1_2 Save your changes and close the editor: :wq Now restart the smtpd service by executing /var/mdw/scripts/smtp restart Note: If you remove SSLv3 and do not turn TLSv1.2 back on, you are left with no HIGH profile ciphers. So ensure that TLSv1.2 is turned back on.
POP3 Proxy	Disable SSLv3 for POP3: Navigate to /var/chroot-pop3/etc/ Open the exim.conf with vi: vi pop3proxy.conf Insert :!SSLv3 to the end of tls_require_ciphers Save your changes and close the editor: :wq Repeat this action for pop3proxy.conf-default Now restart the smtpd service by executing /var/mdw/scripts/pop3 restart
HTTP/HTTPS Proxy	Logon to the shell of the UTM as root Type in cc to access the confd-client Navigate to http | tlsciphers_client$ Now enter the following into the command line to change the ciphers: =ECDHE-RSA-RC4-SHA:ECDHE-ECDSA-RC4-SHA:ECDH-RSA-RC4-SHA:ECDH-ECDSA-RC4-SHA:RC4-SHA:PSK-RC4-SHA:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:ECDH-RSA-AES256-GCM-SHA384:ECDH-ECDSA-AES256-GCM-SHA384:ECDH-RSA-AES256-SHA384:ECDH-ECDSA-AES256-SHA384:ECDH-RSA-AES256-SHA:ECDH-ECDSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:CAMELLIA256-SHA:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDH-RSA-AES128-GCM-SHA256:ECDH-ECDSA-AES128-GCM-SHA256:ECDH-RSA-AES128-SHA256:ECDH-ECDSA-AES128-SHA256:ECDH-RSA-AES128-SHA:ECDH-ECDSA-AES128-SHA:AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:CAMELLIA128-SHA

	The result displayed should look like this: result: 1 127.0.0.1 MAIN http > tlsciphers_client$ ECDHE-RSA-RC4-SHA:ECDHE-ECDSA-RC4-SHA:ECDH-RSA-RC4-SHA:ECDH-ECDSA-RC4-SHA:RC4-SHA:PSK-RC4-SHA:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:ECDH-RSA-AES256-GCM-SHA384:ECDH-ECDSA-AES256-GCM-SHA384:ECDH-RSA-AES256-SHA384:ECDH-ECDSA-AES256-SHA384:ECDH-RSA-AES256-SHA:ECDH-ECDSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:CAMELLIA256-SHA:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDH-RSA-AES128-GCM-SHA256:ECDH-ECDSA-AES128-GCM-SHA256:ECDH-RSA-AES128-SHA256:ECDH-ECDSA-AES128-SHA256:ECDH-RSA-AES128-SHA:ECDH-ECDSA-AES128-SHA:AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:CAMELLIA128-SHA restart the HTTP/HTTPS proxy after you have changed the ciphers: /var/mdw/scripts/httpproxy restart