

Modus™ Verschlüsselung

Einführung

E-Mail wird von Natur aus immer mehr transaktionsbezogen; sie wird verwendet, um mit Angestellten, Kunden und Partnern zu kommunizieren. Heutzutage werden die meisten Informationen, und darunter ein beträchtlicher Anteil an sensiblen Daten, im Klartextformat ohne jeglichen Schutz, also für jedermann lesbar, über das Internet geschickt. Verschiedene Gesetze und Bestimmungen in den Vereinigten Staaten, Europa, und im Rest der Welt spezifizieren, dass einige dieser Daten sicher (verschlüsselt) übermittelt werden müssen. Dies umfasst im Speziellen die öffentliche Hand (Sarbanes-Oxley) und den Gesundheits-Sektor (HIPAA).

Die Lösungen von Modus™ unterstützen eingebaute E-Mail Funktionen für sicheren Client-Zugriff, sicheren Web-Zugriff (WebMail & WebQuarantäne) und die sichere Kommunikation zwischen Mail Servern (inkl. ModusMail), Mail Relays (inkl. ModusGate) und Authentifizierungs-Server.

Technologie-Übersicht

Modus™ kann sicher stellen, dass die E-Mail Transportwege gegen „Sniffer“ und nicht autorisierte Zugriffe geschützt sind – Mitteilungen können nicht während der Übermittlung gestohlen und durch unautorisierte Individuen entschlüsselt werden.

Die Modus™ Technologie von Vircom unterstützt die Verschlüsselung zwischen E-Mail Clients, E-Mail Gateways und E-Mail Server mit der TLS/SSL (128-Bit) Verschlüsselung, um damit das Abhören und Abfangen von Mitteilungen auf dem Transportweg zu unterbinden. Modus™ kann einerseits TLS/SSL Anfragen und die damit verbundenen Zertifikate verarbeiten, und andererseits TLS/SSL Verschlüsselungs-Anfragen an andere Server initiieren, welche dann von diesen verarbeitet werden.

Modus™ kann konfiguriert werden, um verschlüsselte Sessions zu akzeptieren von:

- E-Mail Clients (SMTP, POP3 oder IMAP4 Verschlüsselung wird je nach Bedarf eingeschaltet),
- Web Clients (HTTPS Verschlüsselung gegenüber WebMail oder WebQuarantäne Server),
- Mail Server der Relays (SMTP Verschlüsselung)

Standardmässig initiiert Modus™ verschlüsselte Sessions mit:

- Authentifizierungs-Servern (verwendet TLS über SMTP, POP3 oder Secure LDAP),
- anderen Mail Servern oder Relays (welche TLS über SMTP unterstützen)

Modus™ versucht zuerst eine verschlüsselte Verbindung zu initiieren, und wenn die andere Seite dies nicht unterstützt, wird automatisch eine nicht-verschlüsselte Verbindung aufgebaut:

- Die Art der Verbindung wird pro Server nachgeführt, so dass Modus™ das nächste Mal nicht zuerst eine sichere Verbindung versucht, wenn das Ziel eine solche nicht unterstützt
- Das System entdeckt und korrigiert blockierte Situationen

Auch wenn die Verschlüsselung aktiviert ist, akzeptiert Modus™ trotzdem nicht-verschlüsselte Sessions. Modus™ kann die Verschlüsselung aber bei Bedarf für bestimmte IP-Adressen erzwingen (entweder für eingehende oder für ausgehende Verbindungen). Verbindungen, die mit IP-Adressen in der Liste „Eingehende und ausgehende Verschlüsselung für diese IP-Adressen erzwingen“ gemacht werden, werden abgewiesen, wenn der Client nicht nach einer verschlüsselten Verbindung fragt. Man

muss sich aber bewusst sein, dass es unter Umständen Kompatibilitätsprobleme geben kann, wenn die SMTP-Verschlüsselung aktiviert ist und der andere Server nicht die gleichen Verschlüsselungsprotokolle unterstützt.

Für eine Liste verschiedener IP-Adressen können bei Modus™ jedoch verschiedene Zertifikate verwendet werden. Dies erlaubt es, für verschiedene Domänen und IP-Nummern separate Verschlüsselungen zu verwenden.

Hinweise zur Performanz

Die SSL/TLS Verschlüsselungsroutinen benötigen auf dem Server eine hohe Anzahl von CPU Zyklen. Ein Server verarbeitet zirka zehn mal weniger SSL/TLS Verbindungen als ein Server ohne Verschlüsselungs-Unterstützung. Wenn ein Client eine E-Mail abholt, wird wegen der Verschlüsselung mehr CPU Zeit benötigt. Bei der Verwendung der SSL/TLS Verschlüsselung wird der Betriebssystem-Service LSASS.EXE zusätzliche CPU-Zeit benötigen. Dieser "Local Security Authority Service" prüft die Zertifikate und ihre Gültigkeit.

ModusGate Umgebungen

Übersicht

Das untenstehende Bild zeigt die verschiedenen Verschlüsselungs-Verbindungen auf, die unterstützt werden.

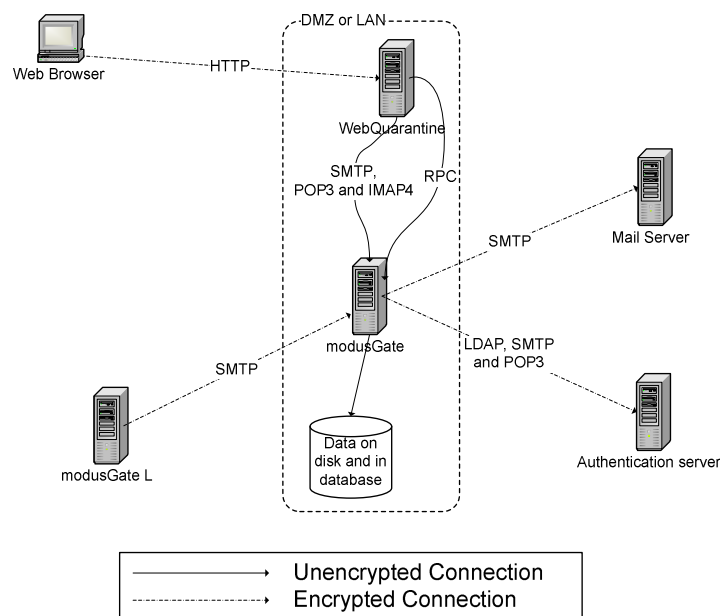


Bild-1: Die ModusGate Verschlüsselungs-Verbindungen

E-Mail Client (Outlook, Eudora...) Verbindungen mit ModusGate

Ein E-Mail Client kann seinen gesamten ausgehenden Verkehr an den ModusGate Relay schicken (zum Beispiel für ausgehende E-Mail Sicherheit) und erhält über den Port 25 eine sichere, verschlüsselte SMTP Verbindung.

Web Browser

Ein Web Browser (Internet Explorer usw.) kann eine sichere (verschlüsselte) HTTPS Verbindung mit der WebQuarantäne auf dem ModusGate Webserver aufbauen.

E-Mail VPN's & Extranet's

Bei grossen Unternehmen kann die gesamte Kommunikation zwischen den verschiedenen ModusGate Servern verschlüsselt werden, damit das Unternehmen an verschiedenen Standorten von den jeweils günstigsten Zugängen zu lokalen Internet Access Providern profitieren kann.

Unternehmen können auch die sichere E-Mail Umgebung auf ihre Kommunikations-Partner ausweiten. Wenn die konventionellen E-Mail Server ihrer Partner keine Verschlüsselung unterstützen, kann eine äusserst kostengünstige ModusGate Version „L“ (ab CHF 650.-) als sicheres Gateway in der Infrastruktur des Partners installiert werden, um die Verschlüsselung zu gewährleisten.

Implementation

Die Konfiguration von ModusGate Zertifikaten

Eine neuer Eintrag "Encryption & Certificates" wurde im Sicherheitsmenü der Modus Konsole eingefügt. Standardmässig ist die Verschlüsselung ausgeschaltet.

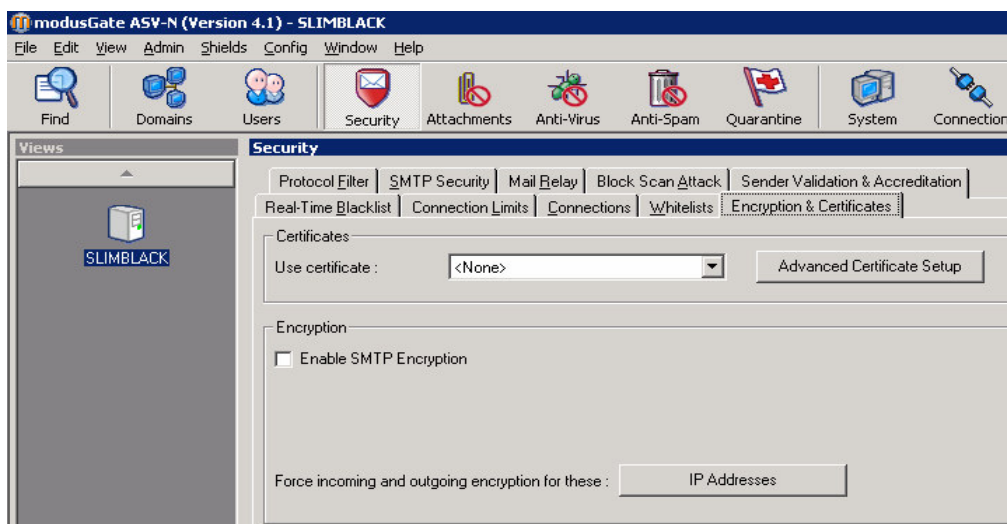


Bild-2: Die Konfiguration von ModusGate Zertifikaten

Um die Verschlüsselung zu aktivieren, muss ein ausgewähltes Zertifikat, das bei einer Zertifikats-Autorität¹ gekauft wurde, eingegeben werden.

Der Bildschirm "Advanced Certificate Setup" (Erweiterte Zertifikats-Einstellungen) erlaubt es, für verschiedene IP-Nummern verschiedene Zertifikate auszuwählen. Dieses hilft beispielsweise ISP's, individuelle Zertifikate für spezielle Domänen zu aktivieren.

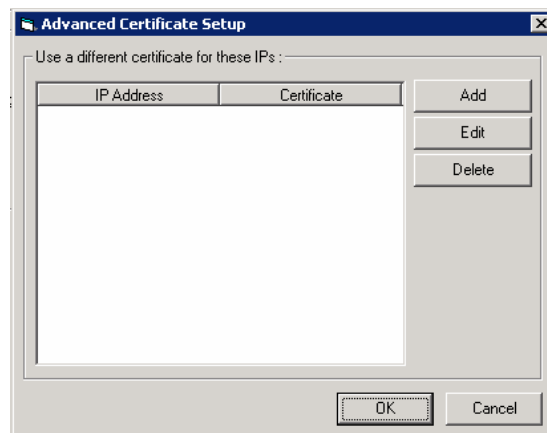


Bild-3: Erweiterte Zertifikats-Einstellungen

Die Aktivierung der SMTP Verschlüsselung erlaubt:

- Die Bearbeitung von STARTTLS Anforderungen von E-Mail Clients, welche ModusGate als Relay benutzen (für ausgehenden E-Mail Verkehr),
- Die Bearbeitung von STARTTLS Anforderungen von einem anderen ModusGate (oder Relay) in einem VPN E-Mail Szenario,
- Initiierung von STARTTLS Anforderungen an andere Mail Server, an die Modusgate sichere E-Mail senden soll (ein definiertes Zertifikat ist hier nicht erforderlich)

Die Verschlüsselung kann für eingehenden und ausgehenden Verkehr von und an verschiedene/n definierte IP-Nummern erzwungen werden.

¹ Der Kaufvorgang und die Importierung von Zertifikaten wird im Anhang erklärt.

Das VPN E-Mail Szenario

Das VPN E-Mail Szenario wird meist in Unternehmen mit geografisch verteilten Standorten eingesetzt. Es erlaubt einem Unternehmen, an jedem Standort kostengünstig regionale Internet Access Provider einzusetzen, und gleichzeitig sicherzustellen, dass der gesamte E-Mail Verkehr, der über das Internet geht, verschlüsselt ist.

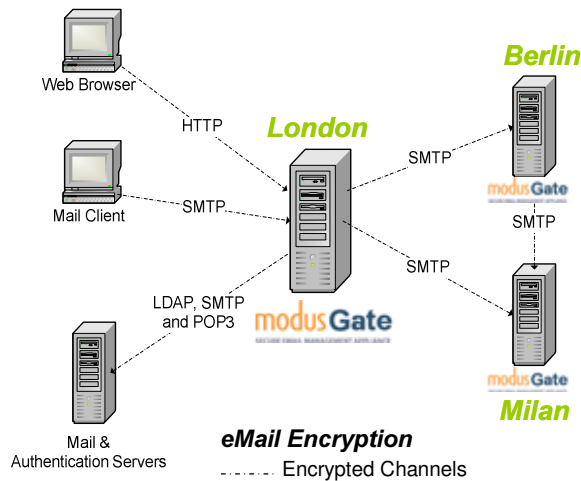


Bild-4: VPM E-Mail

Um dies zu erreichen, braucht man:

- Ein gültiges Zertifikat auf jedem ModusGate Server
- Die SMTP Verschlüsselung auf jedem Modusgate Server aktiviert
- Auf jedem ModusGate Server für alle IP-Nummern der anderen firmeninternen ModusGate Sever die Aktivierung der „zwingenden Verschlüsselung“.

E-Mail Clients

Die verwendete Methode hängt von den Möglichkeiten der E-Mail Clients ab:

Outlook Express

Hier muss man lediglich in der **“Advanced”** Sektion des Benutzerkontos **„SSL”** aktivieren. Die Port Nummer kann bei Bedarf geändert werden.

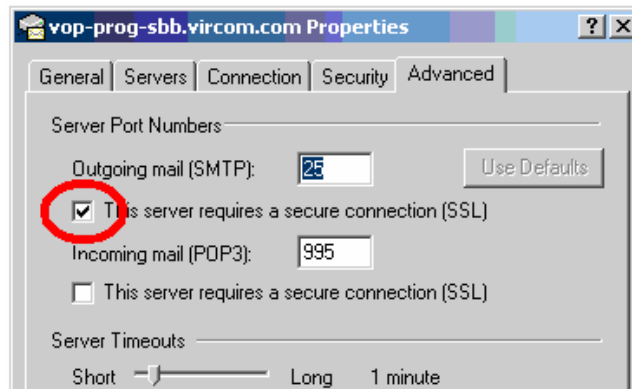


Bild-5: SMTPS Client Einstellung bei Outlook Express

Outlook 2000/XP

Hier muss man lediglich in der Sektion **“More Settings”** auf **“Advanced”** klicken und **„SSL”** aktivieren. Die Port Nummer kann bei Bedarf geändert werden.

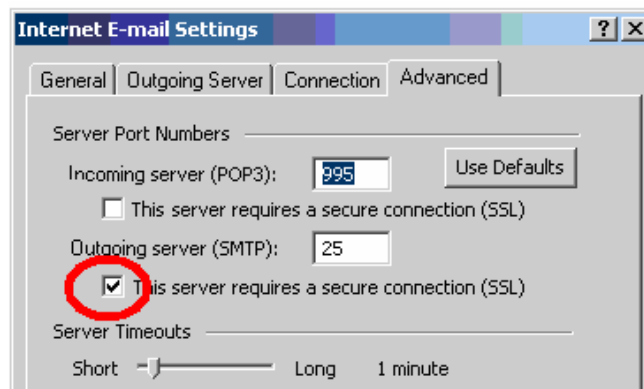


Bild-6: SMTPS Client Einstellung bei Outlook 2000 & XP

WebQuarantine/WebAdmin Clients

WebQuarantine/WebAdmin Clients können über das sichere HTTPS Protokoll auf ModusGate zugreifen. Um dies zu aktivieren, wird ModusGate wie folgt konfiguriert:

- Die Zertifikate der Webserver Maschine müssen im Verzeichnis des Standard-Kontos des lokalen Computers (Client) installiert sein.
- Beim Internet Information Services (IIS) Manager wird die Standard Webseite (oder die spezifische Webseite, für welche die Verschlüsselung installiert werden soll) ausgewählt, dann öffnet man mit der rechten Maustaste die Properties (Einstellungen).
- Verzeichnis-Sicherheits Tab auswählen
- Auf "Edit" klicken
- Die Stärke der gewünschten Verschlüsselung auswählen:
- Die Wahl von „Secure Channel (SSL)“ erfordert, dass die Anwender eine sichere HTTPS Verbindung mit der Modus Web-Applikation aufbauen müssen
- Die Wahl der „128-bit Verschlüsselung“ erfordert, dass die Anwender eine noch stärkere Verschlüsselungsmethode (stronger Encryption) anwenden müssen
- Bei der Sektion „Client Certificates“ muss die Wahl "Ignore client certificates" (Standard-Einstellung) ausgewählt werden.
- Mit dem Anklicken von „OK“ kommt man wieder in das IIS Hauptmenü.

Verschlüsselte Authentifizierung

Im Menü "Connection" können auch die Validation der E-Mail Adressen ("Automatically populate user list") und Authentifizierungs-Sessions verschlüsselt werden. Wie im Bild-7 aufgezeigt, kann die Authentifizierungsmethode pro Domäne ausgewählt und für diese partikuläre Session die Verschlüsselung aktiviert werden. Dies macht die Möglichkeiten vielseitig und flexibel. Die Verschlüsselung wird durch den entsprechenden Authentifizierungs-Server gewährleistet. Um eine Session verschlüsseln zu können, muss der Authentifizierungs-Server ein gültiges Zertifikat installiert haben.

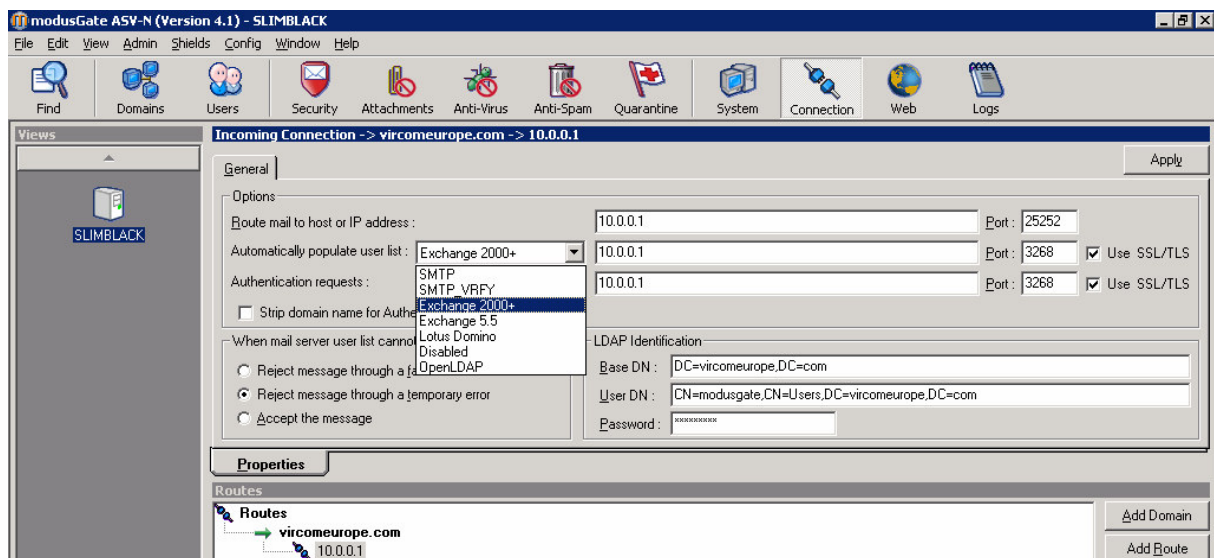


Bild-7: Einstellungen für verschlüsselte Authentifizierung

ModusMail Umgebungen

Übersicht

Das untenstehende Bild zeigt die verschiedenen Verschlüsselungsverbindungen auf, welche ModusMail unterstützt.

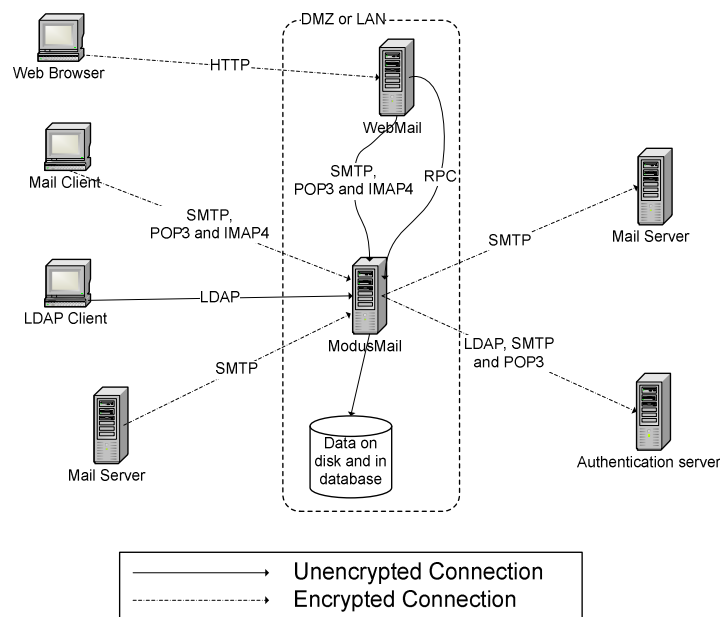


Bild-8: Verschlüsselte Verbindungen mit ModusMail

E-Mail Client (Outlook, Eudora...)

In diesem Fall wird ein E-Mail Client eine sichere (verschlüsselte) Verbindung anfordern. Der E-Mail Client wird so konfiguriert, um im sicheren Modus zu arbeiten. Folglich wird der E-Mail Client eine sichere Verbindung zum Server mittels einer „Sicheren SSL SMTP Verbindung“ über Port 25 und eine sichere Verbindung zum Server mittels einer „Sicheren SSL POP3 Verbindung“ über Port 995 benutzen.

Web Browser

Ein Web Browser (Internet Explorer usw.) kann eine sichere, verschlüsselte HTTPS Verbindung mit der WebQuarantäne auf dem ModusMail Webserver aufbauen.

e-Mail VPN

Die Kommunikation zwischen allen Mail Servern von Unternehmen wird verschlüsselt, vorausgesetzt dass jeder Mail Server TLS/SSL Verschlüsselungs-Anforderungen initiieren und bearbeiten kann.

ETRN Fernabfragen an ModusMail

Hier kontaktiert ein ferner Mail Server (zum Beispiel eines Unternehmens) den ModusMail Server (zum Beispiel eines ISP's), um die E-Mails seiner Domäne herunterzuladen. Die ETRN Anfrage des fernen Servers wird nicht verschlüsselt. Jedoch kann der SMTP Mail Transfer vom ModusMail Server zum fernen Mail Server verschlüsselt stattfinden, wenn der ferne Mail Server dies auch unterstützt.

Implementation

Die Konfiguration von ModusMail

Eine neuer Eintrag "Encryption & Certificates" wurde im Sicherheitsmenü der Modus Konsole eingefügt. Standardmässig ist die Verschlüsselung ausgeschaltet.

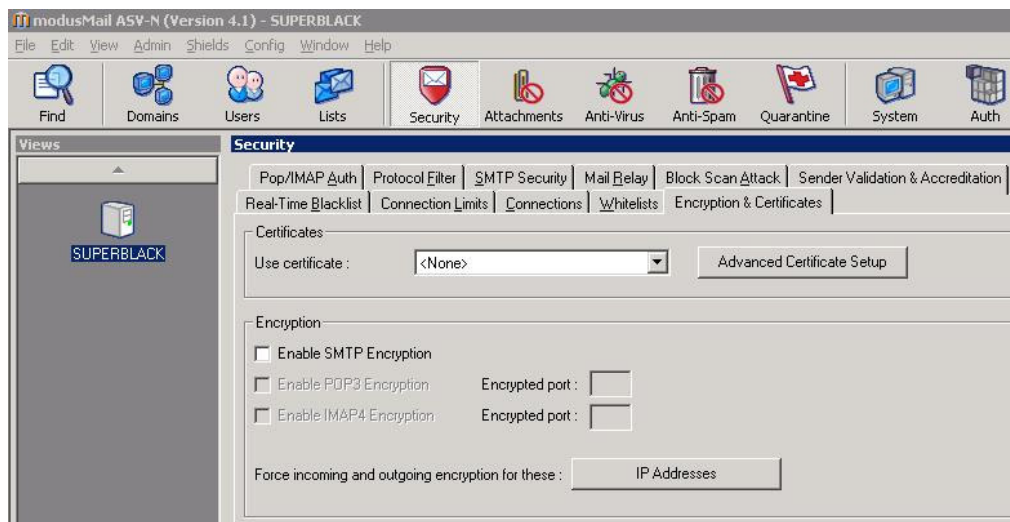


Bild-9: Verschlüsselung & Zertifikat-Einstellungen

Um die Verschlüsselung zu aktivieren, muss ein ausgewähltes Zertifikat eingefügt werden.

Genau wie bei ModusGate (siehe auch Bild-3) erlaubt der "Advanced Certificate Setup" Bildschirm, auf dem ModusMail Server für verschiedene IP-Nummern unterschiedliche Zertifikate auszuwählen. Dies hilft ISPs, für spezielle Domänen individuelle Zertifikate zu verwenden.

Die Aktivierung der SMTP Verschlüsselung erlaubt:

- STARTTLS Anforderungen von Mail Relays (inkl. modusGate) zu verarbeiten, oder dass Mail Clients den ModusMail Server als sicheren Relay verwenden (für ausgehenden Verkehr),
- STARTTLS Anforderungen an andere Mail Server zu initiieren, an welche ModusMail E-Mails übermitteln will (dies benötigt kein definiertes Zertifikat)

Die ModusMail POP3 Verschlüsselung bearbeitet auch POP3S Anforderungen von E-Mail Clients.
Die ModusMail POP3 Verschlüsselung bearbeitet auch IMAP4S Anforderungen von E-Mail Clients.
Die Verschlüsselung kann pro IP-Nummern für ein- und ausgehenden Verkehr erzwungen werden.

E-Mail Clients

Es gibt zwei Arten, um eine sichere POP3 Verbindung für eingehende E-Mail zu etablieren:

1. Verwendung des Portes **995**: Dieser Port wird nur für sichere Verbindungen verwendet. Wenn ein Client mit diesem Port verbunden ist, ist die Verbindung gesichert (verschlüsselt), und die Daten können vertraulich ausgetauscht werden.
2. Verwendung des Portes **110**: Die Verbindung wird im Klartextmodus aufgebaut. Vor dem Einloggen sendet der Client einen „STLS Befehl“ und der Server versucht, die Verbindung zu sichern (verschlüsseln). Wenn dies gelingt, werden die Daten vertraulich ausgetauscht.

Die verwendeten Methoden sind von den Möglichkeiten der Clients abhängig.

Outlook Express:

Hier muss man lediglich in der **“Advanced”** Sektion des Benutzer-Kontos **„SSL“** aktivieren.
Die Port Nummer kann bei Bedarf geändert werden.

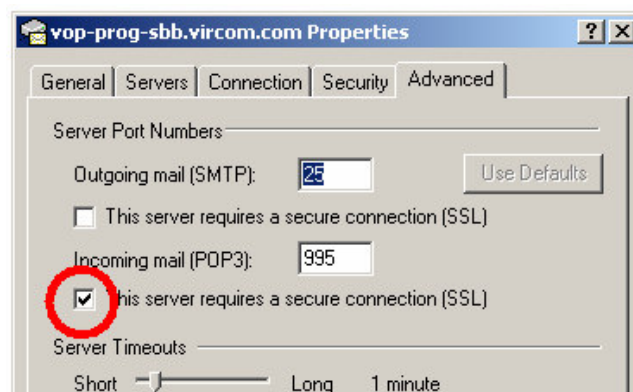


Bild-10: POP3S Client Einstellungen in Outlook Express

Outlook 2000/XP:

Hier muss man lediglich in der Sektion **“More Settings”** auf **“Advanced”** klicken und **„SSL“** aktivieren. Die Port Nummer kann bei Bedarf geändert werden.

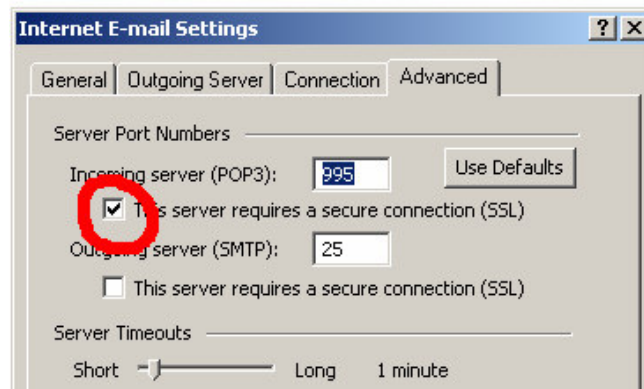


Bild-11: POP3S Client Einstellungen in Outlook 2000 & XP

Qualcomm Eudora:

Der Qualcomm Eudora E-Mail Client unterstützt beide Arten von SSL/TLS. Abhängig von den Server Einstellungen kann die gewünschte Art bei der Sektion **"Incoming mail"** (eingehende E-Mail) ausgewählt werden.

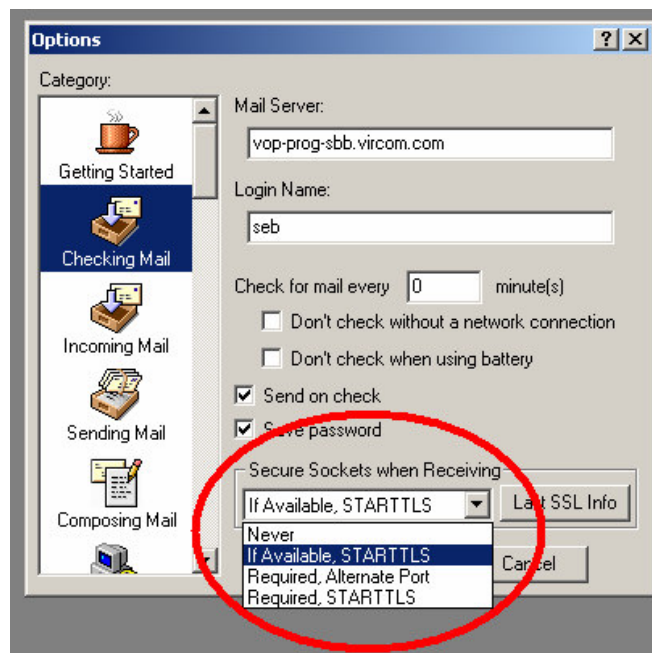


Bild-12: POP3S Client Einstellungen in Eudora

Für ausgehende E-Mails gelten die gleichen Anweisungen zu den SMTPS Verschlüsselungs-Details wie in der ModusGate Sektion in diesem Dokument.

WebMail/WebAdmin Clients

WebMail und WebAdmin Clients können ModusMail via HTTPS erreichen. Dazu wird auf dem ModusMail Webserver die Verschlüsselung aktiviert, wie in der ModusGate Sektion in diesem Dokument beschrieben (WebQuarantine/WebAdmin Clients).

Zusammenfassung

Die gesamte E-Mail Kommunikation kann durch die Modus™ Technologie von Vircom gesichert (verschlüsselt) werden, und zwar:

- Die Kommunikation von E-Mail Clients oder Web Clients
- Die Kommunikation zwischen Mail Servern, Mail Gateways oder beiden
- Die Kommunikation mit darunterliegenden Authentifizierungs-Servern

Anhang

Was sind SSL und TLS?

SSL/TLS wurde geschaffen, um:

- Die Daten zwischen zwei Netzwerk-Endpunkten verschlüsselt zu übermitteln
- Die Authentizität von zwei Endpunkten zu authentifizieren
- Die Integrität der Daten zu gewährleisten

SSL/TLS wird normalerweise benutzt, um über das HTTPS Protokoll mit sicheren Web-Sites wie zum Beispiel Telebanking zu kommunizieren. Es kann aber auch dazu verwendet werden, um andere Arten von verschlüsselten Verbindungen, wie zum Beispiel E-Mail, News oder individueller Datenverkehr) zu gewährleisten.

SSL/TLS Geschichte

SSL (Secured Socket Layer) wurde 1994 von Netscape entwickelt. Die aktuelle Version ist V3. TLS (Transport Layer Security) ist die standardisierte Version von SSL. Der Standard wurde 1999 durch die IETF (Internet Engineering Task Force) fertiggestellt. Technisch ist TLS mit SSL kompatibel.

Prinzipien und Anforderungen, um SSL/TLS benutzen zu können

SSL/TLS ist ein Weg, um Daten zu verschlüsseln und Klartext-Kommunikation zu vermeiden. SSL/TLS benutzt Zertifikate, um die Kommunikation zu verschlüsseln und zu authentifizieren. Zertifikate können von verschiedenen Anbietern wie zum Beispiel Thawte or Verisign² gekauft werden. Diese Firmen werden Zertifikats-Autoritäten genannt. Ein Zertifikat ist eine Datei, welche auf einem Server installiert wird. Aus Sicht des E-Mail Clients sind Zertifikate nicht immer erforderlich, da sie normalerweise auf den Servern verwaltet werden. Meist müssen die Clients entsprechend konfiguriert werden, um mit Zertifikaten arbeiten zu können.

Zertifikate installieren

Um die STARTTLS Anforderungen von E-Mail Clients bearbeiten zu können, muss erst ein Zertifikat gekauft und installiert werden (ein Stück pro Server).

Die Anforderung für ein Zertifikat muss an eine Zertifikat-Autorität geschickt werden. In dieser Anforderung wird der Zertifikat-Autorität mitgeteilt, wer man ist und was man mit dem Zertifikat machen will (in unserem Fall ist das Server-Authentifizierung). Wenn ein Zertifikat angefordert wird, muss diesem ein allgemeiner Name "Common Name" oder „CN“ gegeben werden, und dieser Name muss der DNS-Name (URL) des Servers sein (Beispiel: pop.mycompany.com). Wenn der name nicht mit den DNS-Namenskonventionen übereinstimmt, wird das Zertifikat nicht funktionieren.

Wenn das Zertifikat von der Zertifikats-Autorität akzeptiert wird, stellt es das Zertifikat zur Verfügung.

² Eine detaillierte Liste solcher Firmen gibt es auf <http://www.qmw.ac.uk/~tl6345/ca.htm>

Die Installation des Zertifikates erfordert mehrere Schritte:

1. Das Zertifikat muss auf der Server-Maschine im lokalen Standard Computer Benutzer-Konto installiert werden (Zertifikate MÜSSEN dort installiert werden, sonst kann Modus sie nicht benutzen). Um dies zu machen, wird die Microsoft Management Console (mmc.exe) und die Funktion „**Certificates snap-in**“ verwendet. Mit der Selektion von “Computer Account” können alle Zertifikate angezeigt und die von Zertifikats-Autoritäten erhaltenen Zertifikate importiert werden.
2. Jetzt kann überprüft werden, ob das Zertifikat komplett ist und den privaten Schlüssel (ein Teil des Zertifikates) enthält.

Dies wird im nachfolgenden Bild-13 aufgezeigt:

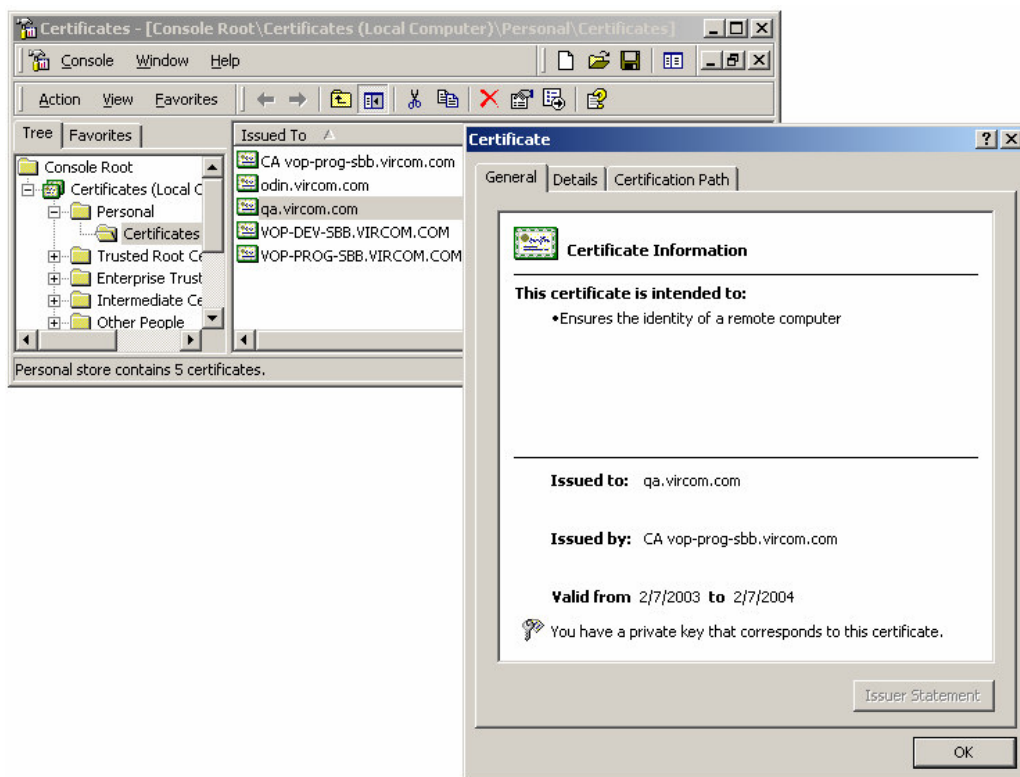


Bild-13: Zertifikat-Einstellungen

Weitere Informationen

Für verschlüsselte Verbindungen benötigte Ports

Es muss beachtet werden, dass die Port Nummern für die Dienste „POP3“, „IMAP4“, „LDAP“ oder „Active Directory Global Catalog Verbindungen“ ändern, und es muss gewährleistet sein, dass diese Ports in den Firewalls geöffnet sind. Die Standard Port Nummern für sichere Verbindungen sind:

- POP3S: 995
- IMAP4S: 993
- LDAPS: 636
- Global Catalog: 3269
- SMTPS: verwendet weiterhin den Port 25, der einzige Unterschied ist, dass der STARTTLS Befehl zu Beginn der Verbindung verwendet wird. Wenn die andere Seite diesen Befehl bestätigt, ist die Verbindung verschlüsselt.

E-Mail Scannen bei Desktop Anti-Virus Programmen ausschalten

Wenn irgendwelche zusätzlichen Desktop Anti-Virus Programme auf dem ModusMail oder ModusGate Server eingesetzt werden, muss die „E-Mail Scan Funktion“ deaktiviert werden. Diese Funktion blockiert alle E-Mail Mitteilungen, welche über eine verschlüsselte Verbindung gesendet werden, weil die Anti-Virus Engine den Inhalt (Body) von verschlüsselten E-Mails nicht untersuchen kann, da er ja verschlüsselt ist. Ausserdem können die Desktop E-Mail Scan Funktionen mit den Scan- und Verarbeitungs-Funktionen von Vircom Moduscan in Konflikt stehen.

GEM 29.09.2005