E-post

Vilka portar används för e-post?

E-postprotokollet, dvs tekniken - eller egentligen de väldigt många olika tekniska funktionerna som används när man skickar och/eller tar emot epost, kan användas på många olika sätt.

Man skiljer även bland annat på att skicka och ta emot epost, som i regel är helt olika metoder..

De vanligaste metoderna för att skicka epost är: SMTP eller Webmail.

SMTP används oftast i ett epostprogram så om du skickar via epostklienten i din dator, telefon eller surfplatta så är det troligen SMTP-tekniken du ska använda.

Du behöver i regel ange ett användarnamn och lösenord för att få möjlighet att skicka utgående epost.

Du behöver även ställa in den port du vill/ska använda för att skicka epostmeddelandet.

I abonnemangsbekräftelsen du fått från oss när du öppnade din eposttjänst så framgår inställningarna du ska använda.

Vanliga portar för SMTP, utgående epost eller eposttrafik som går mellan två olika servrar eller mellan funktioner på en websida och en epostserver är:

Port 25. Detta är standardporten, dvs denna är reserverad för utgående epost.

Tyvärr blockerar vissa Internetoperatörer i Sverige - helt felaktigt - just port 25. Vi har tidigare skrivit artiklar om detta och går inte in på detaljerna här men inte sällan är det tyvär omöjligt att använda port 25 för att skicka utgående epost och då måste man hitta en alternativ väg runt problemet.

Den populäraste metoden är att istället använda port 2525, en port som egentligen inte alls är avsedd för eposttrafik men det ställer i regel inte till några problem att "låna" denna port för eposttrafik istället för port 25.

Vi brukar rekommendera att man alltid använder port 2525 för att slippa ändra mellan olika portar.

Andra funktioner som tex kryptering med certifikat går utmärkt att använda över tex port 2525 så

det finns inte någon anledning att ändra från 2525 heller av denna anledning.

Andra populära portar för utgående eposttrafik är bland annat:

Port 465 - SMTP över SSL (/TLS, dvs krypterad förbindelse).

Denna port används i regel enbart när man skickar epost (som i regel är okrypterad, dvs klartext och teoretiskt möjligt att avlyssna) via en krypterad förbindelse. Oavsett vilken port du använder för att skicka epost kan det vara en god idé att kontrollera att de funktioner som du vill använda, tex kryptering, är inställda på rätt sätt så att du inte tror att trafiken är skyddad när den i själva verket inte är det. Ta gärna hjälp av vår support för att kontrollera att inställningarna är korrekta.

Port 587 - mail submission, RFC 4409. I vissa eposttjänster kan denna port användas förutgående epost mellan ett epostprogram och en epostserver. Kontrollera dokumentationen du fått från oss, det är inte alls säkert att det är möjlight att använda denna port och det är inte bättre eller sämre att använda port 587 än någon annan port, bara annorlunda rent tekniskt.

Port 174 - mailq, används i regel ej. Hantering av epostköer görs idag på ett bättre sätt. Port 174 är idag mycket ovanlig och enbart vissa äldre system som fortfarande står i drift ska använda denna port.

Andra portar som port 50 (Remote Mail Checking Protocol), 209 (Quick Mail Transfer Protocol), 406 (IMSP, Interactive Mail Support Protocol) mfl används i regel inte särskilt ofta. Ta gärna hjälp av vår support för att få hjälp, tips och råd.

Att skicka mail via webmail sker inte via epostprotokollet utan då ansluter du din webläsare via http (vanlig "surfning på webben) eller https (krypterad HTTP-förbindelse, dvs skyddad mot avlyssning) och våra webservrar tar emot förfrågningarna från din webläsare och omvandlar det till epost-trafik.

Befinner du dig på ett nätverk med mycket hög säkerhet och många begränsningar i vilken typ av trafik som får/kan skickas så kan det i värsta fall vara så att webmail är det enda praktiska sättet att skicka epost, om tex all "vanlig" eposttrafik är blockerad i en brandvägg eller liknande.

E-post

Att skicka e-post utan att använda kryptering för att skydda trafiken mellan klient och server är i regel inte farligt, den allra största delen av all eposttrafik på Internet är oskyddad. Nätverken är skyddade på andra sätt och avlyssning är i regel inte ett vanligt förekommande problem.

Därmed inte sagt att man inte behöver krytpering, tvärt om, varför inte använda kryptering på allt som standard bara för att slippa oroa sig över dessa frågor. Att välja kryptering bara på ett enda meddelande är dessutom en dålig metod - då är det ju uppenbart att det är just detta meddelande som är extra känsligt! Om ni använder krytpering på allt så försvinner det extra känsliga meddelandet i mängden och avlyssning blir meningslös.

Vi erbjuder kryptering för såväl utgående som inkommande epost, dvs du kan använda en metod med kryptering när du skickar epost via ditt epostprogram till våra servrar, trafiken "skyddas" och om du skulle befinna dig på ett osäkert trådlöst nätverk på affärsresa exempelvis så behöver du inte oroa dig för att en potentiell "skurk" ska kunna se vad du skickar.

Vi erbjuder även en metod för kryptering när du hämtar epost från våra mailservrar till ditt epostprogram.

Dessutom finns möjligheten att använda webmail med krytpering.

Dessa tre olika metoder skyddar alltså datat (innehållet, tex dina epostmeddelanden) när de överförs mellan din dator och våra servrar. Själva innehållet i epostmeddelandet är i regel ändå i klartext, dvs skulle någon få tillgång till din dator så kan de ändå läsa innehållet.

Om man vill skydda innehållet även mot detta så kan man även välja att när meddelandet skickas kryptera själva innehållet i meddelandet. Här går vi inte in på detaljer kring detta .

Inkommande epost kan också göras på flera olika sätt.

Talar vi om vanlig epost som ska hämtas från våra epostservrar till tex ditt epostprogram i din dator så kan man även här göra det med olika metoder. Den metod som passar de allra flesta är IMAP.

Det finns även andra metoder som tex POP3. Även webmail är såklart möjligt att använda för att läsa epostmeddelanden.

Alla dessa olika metoder kan användas med eller utan kryptering för att skydda datat när det överförs mellan klient och server. Precis som vi beskrivit ovan med SMTP så är detta oberoende av om innehållet i epostmeddelandet är krypterat eller ej utan den kryptering vi talar om här är enbart för att skydda själva överföringen.

E-post

IMAP, som använder port 143, är idag den vanligaste och mest populära metoden för att häta eller läsa epost i ett epostprogram. I princip alla epostklienter som tillverkats de senastee 20 åren har stöd för denna teknik men ibland kan vissa funktioner vara "trasiga" i epostprogrammet, tex för just kryptering.

IMAPs, dvs IMAP över SSL-kryptering går också att använda på port 143. Vissa system föredrar att använda port 220 (avsedd för IMAP 3) för detta vilket också fungerar utmärkt.

En annan vanlig port för IMAP är: 993. Denna port är reserverad för IMAP över SSL. Eftersom det går utmärkt att använda IMAP4-protokollet med kryptering över port 143 så rekommenderar vi istället att man använder port 143 för inkommande epost via IMAP då det är enklare att hålla reda på, särskilt om ni har många datorer, olika nätverk, hemarbetsplatser mm så brukar det vara enklast att hålla koll på två portar: 2525 för utgående epost via krytperad SMTP och inkommande epost via port 143 för krytperad IMAP.

POP3, en av de äldre metoderna för att läsa epost, använder som standard port 110. Vi avråder rent generellt från att använda denna, i många avseenden utdaterad metod, men de användare som vill får självklart använda denna teknik.

POP3s, dvs POP3 över en krypterad förbindelse, använder i regel port 995. I vissa fall stöds överföring via UDP, vi rekommenderar alltid TCP. Kontakta gärna vår support för mer informtion.

POP2, dvs föregångaren till POP3, har vi ej längre stöd för. Detta uråldriga protokoll använde port 109.

Föregångaren till POP2 kallades POP kort och gott och används ej längre.

kPOP, dvs POP över Kerbereos, används mycket sällan men använder port 1109 som standard.

Det finns även andra tekniker för epost som vi inte går in på mer i detalj här. Kontakta gärna vår support för mer information och rådgivning.

Webmail, som använder port 80 för vanlig HTTP (ej krytperad information) eller port 443 för https, dvs krytperad webtrafik, fungerar i regel utmärkt att använda i även enheter som smarta telefoner, surfplattor och många andra terminaler med tillgång till Internet via en webläsare.

Funktioner för att skicka epost från tex webplatser använder ofta också SMTP, detta går vi ej

heller in på i detalj om här utan hänvisar till vår support.

I dokumentationen ni fått från oss framgår i regel hur ni ska ställa in tex funktioner i script eller liknanande för att kunna skicka utgående epost.

Använder er webplat / webshop CCM så behöver ni i regel aldrig komma i kontakt med inställningarna för hur epost skickas.

På vår webplats kan ni läsa mer, vi har även samlat relevanta RFC-dokument där som kan vara praktiska att ha som referens om ni ska ta fram en egen funktion för att hantera epost i tex ett webbaserat verktyg.

Tänk på att epost är ett av de allra krångligaste teknikerna att använda på Internet och mest ansvarsfyllda funktionerna att hantera. Det finns mycket regler kring både teknik och ansvar för administration och liknande. Det finns även många säkerhetsrisker och att jobba med tt tex hantera, erbjuda eller utveckla eposttjänster på Internet är inte någonting vi rekommenderar att man gör, i regel ställer det till allvarliga problem.

Att hantera eposttjänster omfattas även av en rad regler, lagar och riktlinjer.

Sist men inte minst är det kompetenskrävande, resursintensivt och förutsätter att en lång rad underliggande tekniker, funktioner, teknisk infrastruktur mm finns på plats, är designad på ett genomtänkt sätt och underhålls löpande. Inte någonting man vill syssla med på ett vanligt företag med andra ord då felaktigt inställda eposttjänster riskerar kosta både tid, pengar och orsaka problem som är svåra att lösa och går ut över kärnverksamheten. Av denna anledning är det tveklöst mest kostnadseffektivt att anlita en expert som vi på compartment för att hantera företagets eposttjänster. Vi har även lång vana av att hjälpa företag som råkat hamna i problem och vi reder gärna ut er trasiga epostlösning om ni skulle drabbats av detta.

Kort summering:

Behöver du ställa in portar i ditt epostprogram eller på din websida för att skicka och/eller ta emot epost: titta först i abonnemangsbekräftelsen ni fått från oss tidigare (saknar ni denna: kontakta vår support).

Behöver ni använda alternativa portar, ta gärna hjälp av vår support och tänk till innan ni genomför en inställning som "bryter" mot de gällande riktlinjer som finns på Internet.

Används kryptering för att skydda överföring mellan tex server och klient: testa alltid att trafiken verkligen ÄR krytperad. Bara för att du använder en port som är AVSEDD för kryptering så innebär det inte att du verkligen "slagit på" krytperingsfunktionen.

E-post

Används annan krytpering, tex innehåll i ett epostmeddelande eller en annan tjänst som VPN så kontrollera även här att allt fungerar som det ska. Bara för att du kan "skicka" epost så betyder det inte att du är "så säker som du tror".

Vid ev frågor eller funderingar: kontakta alltid vår support. Via våra olika IT-supportavtal och de olika SLA:er som vi erbjuder kan vi alltid garantera er den hjälp ni behöver på ett sätt som passar era behov.

Relaterad information finns även på vår supportsida.

E-post finns både som fristående tjänst hos oss men ingår även i andra tjänster som webhotell. Vi erbjuder även andra eposttjänster som bland annat serverhostingtjänsten

dedikerad egen epostserver, mail-redirect, sekundär mailserver, epostfiltrering mm. Kontakta oss för mer information.

http://www.compartment.se/

Unikt lösnings-ID: #1072
Av: : compartment AB
Senast uppdaterad: 2016-02-02 16:21