Biztonságos FTP támogatása

A hálózatokon keresztül utazó adatokat külső személyek is megfigyelhetik. Ha az adatok magánjellegű információkat, például jelszavakat vagy bankkártyaszámokat tartalmaznak, akkor lépéseket kell tenni, hogy az illetéktelen felhasználók számára ne legyenek értelmezhetők az adatok. Az adattitkosítás kriptográfiai protokollokkal érhető el, mint például a Védett socket réteg (SSL) és a Szállítási réteg biztonság (TLS). Ha FTP protokoll kerül felhasználásra SSL vagy TLS elemmel, akkor a biztonsági mechanizmus neve: biztonságos FTP vagy FTPS (másnéven SSL feletti FTP, vagy TLS feletti FTP).

A Védett socket réteg (SSL) vagy a Szállítási réteg biztonság (TLS) beállításával biztosíthatja az FTP kiszolgáló és az illesztő között küldött információk integritását. Ha az illesztő úgy van beállítva, hogy biztonságos FTP-n működjön, akkor a vezérlőkapcsolat és az adatkapcsolat is titkosítható.

védett socket réteg (SSL)

A Védett socket réteg (SSL) egy hálózati protokoll, amely az adatok biztonságos átvitelére szolgál. Az SSL protokoll a nyilvános kulcsú titkosítást használja az adatok titkosításához az átvitel közben, és az adatok bizalmasságának biztosításához is.

Szállítási réteg biztonság (TLS)

A Szállítási réteg biztonság (TLS) egy protokoll, amely az ügyfél és a kiszolgáló közötti biztonságos adatátvitelt valósítja meg. Ez a Védett socket réteg (SSL) protokoll utódja.

FTPS csatlakozási módok

Az FTPS ügyfél implicit vagy explicit módon alakíthat ki kapcsolatot a biztonságos FTP kiszolgálóval.

Implicit mód: Implicit módban az ügyfél és a kiszolgáló közötti kommunikáció azonnal biztonságos módon kerül beállításra. Az ügyfél és a kiszolgáló között cserélt szöveges információk titkosított formátumban vannak. Az implicit mód alapértelmezett portja a 990.

Explicit mód: Explicit módban a kapcsolat egy titkosítás nélküli FTP kapcsolattal kezdődik. Ha érzékeny információkat (például jelszót) kell elküldeni, akkor az ügyfél explicit módon kiad egy kérést, hogy átváltson biztonságos FTP kapcsolatra. A sikeres SSL egyeztetés után egy biztonságos parancs csatorna kerül kialakításra az ügyfél és a kiszolgáló között.

Az explicit mód az alapértelmezett 21-es porttal működik, és megfelel az RFC 2228 parancsok szabványának. Az RFC 2228 határozza meg a mechanizmust a kapcsolatok hitelesítéséhez és bizalmas adatátvitelekhez a ügyfél és a kiszolgáló között, és ezt hívjuk explicit módnak. Az AUTH paranccsal lehet megadni a biztonsági mechanizmust az explicit mód számára. Az ügyfél egy AUTH parancsot (AUTH SSL/TLS) küld az FTPS kiszolgálónak, és átvált biztonságos parancs kapcsolatra.

A kapcsolatmódok használatával be lehet állítani az adatvédelemi szintet, amellyel az adatok átvitelre kerülnek az ügyfél és a kiszolgáló között.

Adatkapcsolat titkosítás

Az RFC 2228 szerint a Védelmi pufferméret (PBSZ) és Adatcsatorna védelmi szint (PROT) parancsokat az ügyfél adja ki a védelmi szint megadásához az adatcsatornán.

A Védelmi pufferméretttel (PBSZ) a maximális védett pufferméretet egyeztetheti az adatkapcsolat számára. A PBSZ parancs egy hosszú értéket vesz fel argumentumként, és megállapítja a puffer maximális méretét, amelyben a kódolt adatok elküldésre vagy fogadásra kerülnek az adatátvitelek során.

A TLS feletti FTP csak a 0 értékű PBSZ-t támogatja annak biztosításához, hogy ne történjen pufferelés. A '0' argumentumértékkel rendelkező PBSZ parancs egy adatfolyam protokollt jelez, és az adatok egy adatfolyamként kerülnek átvitelre.

A PROT parancs ügyfél/kiszolgáló egyeztetést tesz lehetővé az biztonsági szintű adatkapcsolathoz. Az RFC 2228 a védelem alábbi négy szintjét határozza meg:

1. Üres (C): Az Üres védelmi szint azt jelzi, hogy adatcsatorna fogja szállítani a fájlátvitel nyers adatait, alkalmazott biztonság nélkül.
2. Biztonságos (S): A Biztonságos védelmi szint azt jelzi, hogy az adatok integritása védett.
3. Bizalmas (E): A Bizalmas védelmi szint azt jelzi, hogy az adatok bizalmassága védett.
4. Privát (P): A Privát védelmi szint azt jelzi, hogy az adatok integritása és bizalmassága védett.

A TLS feletti FTP protokoll csak az adatvédelem Üres és Privát szintjeit támogatja.

Kiszolgáló hitelesítés

A kiszolgáló hitelesítés a biztonságos kapcsolathoz elvégzett ellenőrzés. Miközben kialakít egy SSL kapcsolatot az FTPS kiszolgálóval, az FTP ügyfél elvégzi a kiszolgáló tanúsítvány érvényesítést az ügyfél kulcsadatbázisban található tanúsítványokkal. Az ügyfél kulcsadatbázis az összes megbízható kiszolgáló tanúsítványát tartalmazza. Ha a kiszolgáló szükséges tanúsítványa megtalálható az ügyfél kulcsadatbázisában, akkor a kapcsolat kialakításra kerül.

Ha a tanúsítvány nem található az ügyfél kulcsadatbázisban, akkor a rendszer a kiszolgálót megbízhatatlan kiszolgálónak tekinti, és egy kivétel kerül előállításra, és nem lehet kapcsolatot kialakítani az FTPS kiszolgálóval.

Ügyfél hitelesítés

Az ügyfél hitelesítés hasonló kiszolgáló hitelesítéshez azzal a különbséggel, hogy a kiszolgáló tanúsítványt kér az ügyféltől annak ellenőrzéséhez, hogy megbízható ügyféltől származik. A tanúsítványt olyan tanúsítványhatóságnak kell aláírnia, amelyet a kiszolgáló megbízhatónak tart. Az ügyfél hitelesítés egy kompatibilis FTPS kiszolgálót igényel a hitelesítéshez. Amikor egy kiszolgáló tanúsítványt kért, az ügyfélnek lehetősége van egy tanúsítvány elküldésére. A kiszolgáló akkor engedélyezi a kapcsolatot, ha az ügyfél tanúsítványa megbízható.

Az FTP kiszolgáló a nyilvános tanúsítvány alapján hitelesíti az ügyfelet, miközben kialakít egy SSL kapcsolatot. Az ügyfél biztosítja a nyilvános kulcsot az SSL kapcsolat során, és ez kicserélésre kerül az FTPS kiszolgálóval, amely hitelesíti az ügyfél azonosságát a kiszolgáló megbízható tanúsítványaiban beállított tanúsítványok alapján.

1. Illesztő beállítása biztonságos FTP használatára (védett socket réteg vagy szállítási réteg biztonság)
   A WebSphere Adapter for FTP támogatja a biztonságos FTP kiszolgálóhoz (FTPS) történő csatlakozást az SSL vagy TLS protokoll használatával. A WebSphere Adapter for FTP beállítható úgy, hogy explicit vagy implicit módon csatlakozzon az FTPS kiszolgálóhoz. Az illesztő a biztonságos FTP-t az SSL 3.0 változattal és a TLS 1.0 változattal támogatja.
2. 140-2-es szövetségi információ-feldolgozási szabványnak megfelelő feldolgozás beállítása az illesztőn
   Az Egyesült Államok kormányzata által elfogadott 140-2-es szövetségi információ-feldolgozási szabvány a szoftvertermékek és modulok kriptográfiai szolgáltatásait szabályozza. Ezek közé a szolgáltatások közé tartozik például a titkosítás, a visszafejtés, a kivonatkészítés (üzenetkivonatok), a védett socket rétegek, az átviteli réteg biztonsága, az internetes protokollok biztonsága, az SSH, az aláírások, a kulcscsere valamint a kulcsok és tanúsítványok előállítása. Azok az Egyesült Államok államigazgatásával együttműködő felhasználók, akiknek teljesíteniük kell az FIPS szabvány előírásait, beállíthatják az illesztőt úgy, hogy az FIPS módban fusson.