Lizenzbestimmungen

include:free_version

Dieser Artikel bietet einen kurzen, kompakten Überblick über die Authentifizierung auf Basis von IEEE 802.1X in Wireless LANs (Enterprise Mode).

IEEE 802.1X - Enterprise Mode (WLAN)

Der Enterprise Mode stellt eine flexible Authentifizierung für Wireless LAN nach dem Standard IEEE 802.1X zur Verfügung und ist damit quasi der große Bruder des Consumer Mode.[1)] In diesem Standard spielt der Accesspoint bei der Authentifizierung nur noch eine untergeordnete Rolle - er wird „Authenticator“ genannt und führt die Authentifizierung nicht mehr selbst durch, sondern ist nur noch ein Vermittler zwischen dem einbuchenden Client (dem „Supplicant“) und einem Server im internen Netz (dem „Authentication Server“).

D.r Auth.nticator v.rwirft all. Pak.t., di. .r von .in.m noch nicht auth.ntifizi.rt.n Cli.nt .mpfängt - .. ..i d.nn .. hand.lt .ich um di. pa…nd.n Pak.t. .in.. Anm.ld.vorgang.. Für d.n Tran.port d.r Auth.ntifizi.rung.information.n zwi.ch.n Supplicant und Auth.nticator .chr.ibt IEEE 802.1X da. Protokoll EAPoL (Ext.n.ibl. Auth.ntication Protocol ov.r LAN) vor[2)]. EAPoL i.t .in ..hr .infach aufg.baut.. Protokoll, da. nur Punkt-zu-Punkt-V.rbindung unt.rhalt.n und damit l.icht abg..ich.rt w.rd.n kann.

Di. EAPoL-Pak.t. d.. Supplicant w.rd.n vom Auth.nticator .ntg.g.n g.nomm.n, in .in and.r.. Protokoll g.kap..lt bzw. umg…tzt und an d.n Auth.ntication S.rv.r im int.rn.n N.tz w.it.r g.l.it.t. IEEE 802.1X .chr.ibt hi.r k.in V.rfahr.n vor und .mpfi.hlt l.diglich d.n Ein.atz d.. RADIUS-Protokoll. und .in.. RADIUS-S.rv.r.. Antwort.n d.. Auth.ntication S.rv.r w.rd.n vom Auth.nticator .nt.pr.ch.nd b.hand.lt, .o da.. .in. Auth.ntifiz.rung zwi.ch.n Supplicant und Auth.ntication S.rv.r .tattfind.n kann ohn. da.. d.r Supplicant Zugang zum int.rn.n N.tz b..itzt.

B.. WPA(2) w.rd.n .m Zug. ..n.r .rfolgr..ch.n Auth.nt.f.z..rung zw..ch.n Acc…po.nt und Cl..nt Schlü…l .u.g.h.nd.lt bzw. vom Acc…po.nt .n d.n Cl..nt w..t.rg.g.b.n. Nur j.n. D.t.n, d.. m.t d.m korr.kt.n Schlü…l v.r.chlü…lt wurd.n, könn.n von Suppl.c.nt und Auth.nt.c.tor .nt.chlü…lt und w..t.rv.r.rb..t.t w.rd.n. So w.rd ..ch.r g..t.llt, d… nur b.r.cht.gt. St.t.on.n m.t d.r Infr..truktur kommun.z..r.n könn.n.

IEEE 802.1x .nd IEEE 802.11. l.g.n n.r d.n g.n.r.ll.n A.fb.. d.r A.th.nt.f.z..r.ng .nd ..n.n T..l d.r v.rw.nd.t.n Pr.t.k.ll. f..t. B..d. St.nd.rd. ..g.n n.cht. .b.r d.. A.th.nt.f.z..r.ng.v.rf.hr.n (..ch EAP-M.th.d. g.n.nnt) …, d.. zw..ch.n S.ppl.c.nt .nd A.th.nt.c.t..n S.rv.r d.rchg.f.hrt w.rd. Akt..ll ..nd h..r m.hr .l. 30 v.r.ch..d.n. V.rf.hr.n .n RFC d.f.n..rt .nd .nz.hl.g. w..t.r. v.n v.r.ch..d.n.n H.r.t.ll.rn .l. pr.pr..t.r. M.th.d.n .mpl.m.nt..rt w.rd.n, d.r.nt.r M.th.d.n, d.. b.n.tz.rb….rt., m.hr.t.f.g. .d.r h.rdw.r.b….r.nd. A.th.nt.f.z..r.ng (T.k.n, SIM-K.rt. .tc.) .rm.gl.ch.n. D.. W.-F. All..nc. z.rt.f.z..rt …t 2009 d.. f.lg.nd.n EAP-M.th.d.n:

B.z..chn.n.	**RFC**	**V.rf.hr.n**
EAP-TLS	RFC 5216	Zw..ch.. S…..c… … A..h….c….. S.rv.r w.r. …. TLS-V.rb…… …..b…. D.r S…..c… w…. ..ch … ….. Z.r….k.. ….
EAP-TTLS/MS-CHAPv2	RFC 5281	Zw..ch.. S…..c… … A..h….c….. S.rv.r w.r. …. TLS-V.rb…… …..b…. Üb.r … TLS-V.rb…… …… …. w….r. A..h……z..r… (..ch „….r. A..h……z..r…“ …….) … H…. v.. U..r…. … P…w.r. ….. (MS-CHAPv2).
PEAPv0/EAP-MSCHAPv2	Dr…	Äh…ch w.. EAP-TTLS.
PEAPv1/EAP-GTC	-	Pr..r….r.. Pr…k… v.. CISCO. Üb.r …. TLS-V.rb…… …… …. ….r. A..h……z..r… .b.r …. G…r.c T.k.. C.r. (H.r.w.r.) ……

B.z..chn.n.	**RFC**	**V.rf.hr.n**
EAP-SIM	RFC 4186	A..h.....z..r... .r..... .b.r .... SIM-K.r...
EAP-AKA	RFC 4187	A..h.....z..r... .r..... .b.r ... UMTS SIM-K.r.. (UMTS A..h....c..... ... K.y A.r.....)
EAP-FAST	RFC 4851	Pr...k... v.. CISCO („F..x.b.. A..h....c..... v.. S.c.r. T.....“), h.....ch. D...r.b..... v.. Sch.....

E.. ....r Üb.rb..ck .b.r ... h..... EAP-M..h.... ....ch ..r .....r.ch..... .....ch..r.ch.... S.... v.. W.k..... .....h....

<.... ....r....> D.r E...r.r... M... ....r ....z. w.r..., w... ... G.r... ....v..... ...h.....z..r. ... v.rw..... w.r... .....:

1. E. ... .r... ..r M.... ..r G.r... ..ch. ..hr .....ch, ... Üb.rb..ck z. b.h.....
2. E. h.rr.ch. ... . K..... ... G.h.. v.. ..b.... G.r.....
3. D.. ..b.... G.r... b..... ..ch .b.r ....r.. Z...r... h..w.. .. ..ch. v.r.r.....w.r..... H..... S.. w.r... z.B. v.r...h.. ...r ... N..z.r ..r G.r... ..h.r.. z.T. ..ch. z.r V.rw..... bzw. z.. U...r..h....
4. ...

</....>

Schw.ch..... E...r.r... M...

D.r E...r.r... M... b..... ... M....chk... ... .r ...z.. R..h. v.. A..h.....z..r..... ... j.w.... ....z.w.h.... L....r b..... ..ch ....r ... .b..... V.r..hr.. ....z. R..h. v.. ....ch.r.. A..h.....z..r.....

<.... ....> D.. A..w.h. ..r EAP-M..h... .... ..r..... v.r..... w.r.... D.. .... A..h.....z..r..... b..... .... h.h. S.ch.rh...:

- EAP-TLS
- EAP-TTLS-PAP/CHAP/MS-CHAP/MS-CHAPv2
- EAP/PEAPv0-TLS/MS-CHAPv2

</....>

b....r....r....h....c.....-..rv.r N.ch ..r A..w.h. ..r EAP-M..h.... .... b.....r.. A.....rk ... ..r.. K.....r..... ..... w.r.... A... b..... K..... (... ..b.... G.r..., ..r Acc..... ... ..r A..h.....z..r.....rv.r) ....r..... k.....r..r. w.r..., ... S.ch.rh... ..r IT-I..r...r.k..r ..ch. z. ....hr.... B.....r. w.ch... ... ..b.., ...b.... G.r... v.r..ch.., ..ch ....ch...ß..ch b.. ..r r.ch..... I..r...r.k..r ..z..... D...r .... ..r C..... .. ..r L... ...., ... A..h.....z..r.....rv.r ...b.. ..... z. ...h.....z..r.., b.v.r .r .h. kr....ch. I...r..... .b.r..b.. A..... b....h. ... G...hr, ... A..r....r ..... v.r..r.. w.r..

<.... ....r....>

- D.r A..h.....z..r.....rv.r .... SSL-Z.r....k.. ....
- D.. C..... .... SSL-Z.r....k.. .r....:
  - D.r S.rv.r.... .. Z.r....k.. ....r... w.r....
  - D.r A.....r ... Z.r....k... ....r... w.r....
  - D.. ..... CA .... v.. C..... ... v.r.r.....w.r... .....h.. w.r....

</....>

..c....:.....r&.......r

include:free_version

1)
IEEE 802.1X definiert den generellen Aufbau einer Authentifizierung und Autorisierung von Clients in IEEE 802-Netzen, definiert das Protokoll EAPoL (Extensible Authentication Protocol over LAN) und empfiehlt den Einsatz von RADIUS. Deshalb wird der Enterprise Mode auch häufig WPA(2)-EAPoL, WPA(2)-EAP, WPA(2)-RADIUS oder WPA(2)-802.1X genannt.

2)
EAPoL war ur.prünglich nur für Eth.rn.t-LAN. g.dacht, wurd. ab.r mit .in.r R.vi.ion d.. Standard. 2004 auf .in. ganz. R.ih. w.it.r.r LAN-T.chnologi.n (unt.r and.r.m auf WLAN) au.g.w.it.t.