Domande frequenti su Cisco Aironet Wireless Security

Sommario

Introduzione

Questo documento offre informazioni sulle domande più frequenti (FAQ) su Cisco Aironet Wireless Security.

Domande frequenti (FAQ)

D. Qual è la necessità di sicurezza wireless?

R. In una rete cablata, i dati rimangono nei cavi che collegano i dispositivi terminali. Ma le reti wireless trasmettono e ricevono dati attraverso la trasmissione di segnali RF all'aria aperta. A causa della natura del broadcast che le WLAN utilizzano, esiste una minaccia maggiore di hacker o intrusi che possono accedere ai dati o danneggiarli. Per risolvere questo problema, tutte le WLAN richiedono l'aggiunta di:

1. Autenticazione utente per impedire l'accesso non autorizzato alle risorse di rete.
2. Privacy dei dati per proteggere l'integrità e la privacy dei dati trasmessi (detta anche crittografia).

D. Quali sono i diversi metodi di autenticazione definiti dallo standard 802.11 per le LAN wireless?

R. Lo standard 802.11 definisce due meccanismi di autenticazione dei client LAN wireless:

1. Autenticazione aperta
2. Autenticazione con chiave condivisa

Esistono anche altri due meccanismi comunemente usati:

1. Autenticazione basata su SSID
2. Autenticazione indirizzo MAC

D. Che cos'è l'autenticazione aperta?

R. L'autenticazione aperta è fondamentalmente un algoritmo di autenticazione nullo, il che significa che non c'è alcuna verifica dell'utente o del computer. L'autenticazione aperta consente a qualsiasi dispositivo di inviare una richiesta di autenticazione al punto di accesso (AP). L'autenticazione aperta utilizza la trasmissione in chiaro per consentire a un client di associarsi a un punto di accesso. Se non è abilitata la crittografia, qualsiasi dispositivo che conosce l'SSID della WLAN può accedere alla rete. Se il protocollo WEP (Wired Equivalent Privacy) è abilitato sull'access point, la chiave WEP diventa un mezzo di controllo dell'accesso. Un dispositivo che non dispone della chiave WEP corretta non può trasmettere dati tramite il punto di accesso anche se l'autenticazione ha esito positivo. Inoltre, un dispositivo di questo tipo non può decrittografare i dati inviati dall'access point.

D. Quali passaggi comporta l'autenticazione aperta per consentire al client di associarsi all'access point?

1. Il client invia una richiesta di richiesta ai punti di accesso.
2. I punti di accesso restituiscono le risposte alle richieste.
3. Il client valuta le risposte del punto di accesso e seleziona il punto di accesso migliore.
4. Il client invia una richiesta di autenticazione all'access point.
5. L'access point conferma l'autenticazione e registra il client.
6. Il client invia quindi una richiesta di associazione all'access point.
7. L'access point conferma l'associazione e registra il client.

D. Quali sono i vantaggi e gli svantaggi dell'autenticazione aperta?

R. Ecco i vantaggi e gli svantaggi dell'autenticazione aperta:

Vantaggi: Autenticazione aperta è un meccanismo di autenticazione di base che è possibile utilizzare con periferiche wireless che non supportano algoritmi di autenticazione complessi. L'autenticazione nella specifica 802.11 è orientata alla connettività. I requisiti per l'autenticazione consentono ai dispositivi di accedere rapidamente alla rete. In questo caso, è possibile utilizzare Autenticazione aperta.

Svantaggi: L'autenticazione aperta non consente di verificare se un client è un client valido e non un client hacker. Se non si utilizza la crittografia WEP con l'autenticazione aperta, qualsiasi utente che conosce l'SSID della WLAN può accedere alla rete.

D. Che cos'è l'autenticazione con chiave condivisa?

R. L'autenticazione a chiave condivisa funziona in modo simile all'autenticazione aperta con una differenza principale. Quando si utilizza l'autenticazione aperta con la chiave di crittografia WEP, la chiave WEP viene utilizzata per crittografare e decrittografare i dati, ma non per la fase di autenticazione. In Autenticazione con chiave condivisa viene utilizzata la crittografia WEP per l'autenticazione. Analogamente all'autenticazione aperta, l'autenticazione a chiave condivisa richiede che il client e l'access point abbiano la stessa chiave WEP. L'access point che usa l'autenticazione a chiave condivisa invia un pacchetto di testo di richiesta al client. Il client utilizza la chiave WEP configurata localmente per crittografare il testo della richiesta di verifica e rispondere con una richiesta di autenticazione successiva. Se l'access point può decrittografare la richiesta di autenticazione e recuperare il testo originale della richiesta di verifica, risponde con una risposta di autenticazione che concede l'accesso al client.

D. Quali passaggi prevede l'autenticazione a chiave condivisa per consentire al client di associarsi all'access point?

1. Il client invia una richiesta di richiesta ai punti di accesso.
2. I punti di accesso restituiscono le risposte alle richieste.
3. Il client valuta le risposte del punto di accesso e seleziona il punto di accesso migliore.
4. Il client invia una richiesta di autenticazione all'access point.
5. L'access point invia una risposta di autenticazione che contiene il testo della richiesta non crittografato.
6. Il client cripta il testo della richiesta con la chiave WEP e lo invia all'access point.
7. L'access point confronta il testo non crittografato della richiesta con il testo crittografato della richiesta. Se l'autenticazione è in grado di decrittografare e recuperare il testo originale della richiesta, l'autenticazione ha esito positivo.

L'autenticazione a chiave condivisa utilizza la crittografia WEP durante il processo di associazione del client.

D. Quali sono i vantaggi e gli svantaggi dell'autenticazione a chiave condivisa?

R. Nell'autenticazione a chiave condivisa, il client e l'access point si scambiano il testo della richiesta (testo non crittografato) e la richiesta crittografata. Pertanto, questo tipo di autenticazione è vulnerabile agli attacchi man-in-the-middle. Un hacker può ascoltare la sfida non crittografata e la sfida crittografata ed estrarre la chiave WEP (chiave condivisa) da queste informazioni. Quando un hacker conosce la chiave WEP, l'intero meccanismo di autenticazione viene compromesso e l'hacker può accedere alla rete WLAN. Questo è lo svantaggio principale dell'autenticazione con chiave condivisa.

D. Che cos'è l'autenticazione dell'indirizzo MAC?

R. Sebbene lo standard 802.11 non specifichi l'autenticazione dell'indirizzo MAC, le reti WLAN in genere utilizzano questa tecnica di autenticazione. Pertanto, la maggior parte dei fornitori di dispositivi wireless, incluso Cisco, supporta l'autenticazione dell'indirizzo MAC.

Nell'autenticazione dell'indirizzo MAC, i client vengono autenticati in base all'indirizzo MAC. Gli indirizzi MAC dei client vengono verificati rispetto a un elenco di indirizzi MAC memorizzati localmente nell'access point o su un server di autenticazione esterno. L'autenticazione MAC è un meccanismo di protezione più avanzato rispetto alle autenticazioni con chiave aperta e condivisa fornite da 802.11. Questa forma di autenticazione riduce ulteriormente la probabilità che periferiche non autorizzate possano accedere alla rete.

D. Perché l'autenticazione MAC non funziona con Wi-Fi Protected Access (WPA) nel software Cisco IOS versione 12.3(8)JA2?

R. L'unico livello di sicurezza per l'autenticazione MAC è controllare l'indirizzo MAC del client in base a un elenco di indirizzi MAC consentiti. Questo è considerato molto debole. Nelle versioni software Cisco IOS precedenti, era possibile configurare l'autenticazione MAC e WPA per crittografare le informazioni. Tuttavia, poiché lo stesso WPA ha un indirizzo MAC per il controllo, Cisco ha deciso di non consentire questo tipo di configurazione nelle versioni software Cisco IOS più recenti e ha deciso solo di migliorare le funzionalità di sicurezza.

D. È possibile utilizzare SSID come metodo per autenticare i dispositivi wireless?

R. SSID (Service Set Identifier) è un valore alfanumerico univoco, con distinzione tra maiuscole e minuscole, utilizzato dalle WLAN come nome di rete. L'SSID è un meccanismo che consente la separazione logica delle LAN wireless. SSID non fornisce alcuna funzione di privacy dei dati né autentica realmente il client nell'access point. Il valore SSID viene trasmesso come testo non crittografato in beacon, richieste di verifica, risposte di verifica e altri tipi di frame. Un intercettatore può determinare facilmente l'SSID utilizzando un analizzatore di pacchetti LAN wireless 802.11, ad esempio Sniffer Pro. Cisco sconsiglia di utilizzare il SSID come metodo per proteggere la rete WLAN.

D. Se si disabilita la trasmissione SSID, è possibile migliorare la sicurezza su una rete WLAN?

R. Quando si disabilita la trasmissione SSID, SSID non viene inviato nei messaggi beacon. Tuttavia, in altri frame, ad esempio Richieste di verifica e Risposte di verifica, l'SSID rimane in testo non crittografato. Pertanto, non è possibile ottenere una protezione wireless avanzata se si disattiva l'SSID. L'SSID non è progettato, né destinato all'uso, come meccanismo di sicurezza. Inoltre, se si disabilitano le trasmissioni SSID, si possono verificare problemi di interoperabilità Wi-Fi per le distribuzioni client miste. Cisco sconsiglia pertanto di utilizzare il SSID come modalità di sicurezza.

D. Quali sono le vulnerabilità rilevate nella protezione 802.11?

A. Le principali vulnerabilità della sicurezza 802.11 possono essere riassunte come segue:

- Autenticazione solo dispositivo debole: I dispositivi client vengono autenticati, non gli utenti.
- Crittografia dei dati debole: Il protocollo WEP (Wired Equivalent Privacy) si è dimostrato inefficace per crittografare i dati.
- Nessuna integrità del messaggio: Il valore di controllo dell'integrità (ICV) si è dimostrato inefficace per garantire l'integrità dei messaggi.

D. Qual è il ruolo dell'autenticazione 802.1x nella rete WLAN?

R. Per risolvere le lacune e le vulnerabilità della sicurezza nei metodi di autenticazione originali definiti dallo standard 802.11, il framework di autenticazione 802.1X è incluso nella bozza per i miglioramenti alla sicurezza del layer MAC 802.11. Il Task Group i (TGi) di IEEE 802.11 sta sviluppando questi miglioramenti. Il framework 802.1X fornisce al livello di collegamento l'autenticazione estensibile, normalmente visibile solo nei livelli superiori.

D. Quali sono le tre entità definite dal framework 802.1x?

R. Il framework 802.1x richiede queste tre entità logiche per convalidare i dispositivi su una rete WLAN.

1. **Supplicant**: il supplicant risiede sul client LAN wireless ed è anche noto come client EAP.
2. **Autenticatore**: l'autenticatore risiede nell'access point.
3. **Server di autenticazione**: il server di autenticazione risiede sul server RADIUS.

D. Come avviene l'autenticazione di un client wireless quando si utilizza il framework di autenticazione 802.1x?

R. Quando il client wireless (client EAP) diventa attivo, il client wireless esegue l'autenticazione aperta o condivisa. 802.1x funziona con l'autenticazione aperta e viene avviato dopo che il client è stato associato correttamente all'access point. La stazione client può associarsi, ma può passare il traffico di dati solo dopo la corretta autenticazione 802.1x. Di seguito sono riportati i passaggi dell'autenticazione 802.1x:

1. Il punto di accesso (autenticatore) configurato per 802.1x richiede l'identità dell'utente al client.
2. I client rispondono con la propria identità entro un periodo di tempo stabilito.
3. Il server controlla l'identità dell'utente e inizia l'autenticazione con il client se l'identità dell'utente è presente nel database.
4. Il server invia un messaggio di operazione riuscita all'access point.
5. Una volta autenticato il client, il server inoltra la chiave di crittografia all'access point che viene utilizzato per crittografare/decrittografare il traffico inviato al client e da esso proveniente.
6. Nel passaggio 4, se l'identità dell'utente non è presente nel database, il server interrompe l'autenticazione e invia un messaggio di errore all'access point.
7. Il punto di accesso inoltra il messaggio al client, che deve ripetere l'autenticazione con le credenziali corrette.

Nota: durante l'autenticazione 802.1x, AP inoltra semplicemente i messaggi di autenticazione da e per il client.

D. Quali sono le diverse varianti EAP che è possibile utilizzare con il framework di autenticazione 802.1x?

R. 802.1x definisce la procedura per autenticare i client. Il tipo EAP utilizzato nel framework 802.1x definisce il tipo di credenziali e il metodo di autenticazione utilizzati nello scambio 802.1x. Il framework 802.1x può utilizzare una delle seguenti varianti EAP:

- EAP-TLS—Extensible Authentication Protocol Transport Layer Security
- EAP-FAST: autenticazione flessibile EAP tramite tunnel protetto
- EAP-SIM - Modulo EAP Subscriber Identity
- Cisco LEAP: Lightweight Extensible Authentication Protocol
- EAP-PEAP: protocollo EAP (Protected Extensible Authentication Protocol)

- EAP-MD5—EAP-Message Digest Algorithm 5
- EAP-OTP: password EAP puntuale
- EAP-TTLS: sicurezza a livello di trasporto con tunnel EAP

D. Come scegliere un metodo EAP 802.1x tra le diverse varianti disponibili?

R. Il fattore più importante da considerare è la compatibilità del metodo EAP con la rete esistente. Cisco consiglia inoltre di scegliere un metodo che supporti l'autenticazione reciproca.

D. Che cos'è l'autenticazione EAP locale?

R. EAP locale è un meccanismo in cui il WLC agisce come server di autenticazione. Le credenziali utente vengono archiviate localmente sul WLC per autenticare i client wireless, che fungono da processo back-end negli uffici remoti quando il server non funziona. Le credenziali utente possono essere recuperate dal database locale sul WLC o da un server LDAP esterno. LEAP, EAP-FAST, EAP-TLS, PEAPv0/MSCHAPv2 e PEAPv1/GTC sono autenticazioni EAP diverse supportate da EAP locale.

D. Che cos'è Cisco LEAP?

R. Lightweight Extensible Authentication Protocol (LEAP) è un metodo di autenticazione proprietario di Cisco. Cisco LEAP è un tipo di autenticazione 802.1X per reti LAN wireless (WLAN). Cisco LEAP supporta l'autenticazione reciproca sicura tra il client e un server RADIUS tramite una password di accesso come segreto condiviso. Cisco LEAP fornisce chiavi di crittografia dinamiche per utente e per sessione. LEAP è il metodo meno complicato per distribuire 802.1x e richiede solo un server RADIUS. Per informazioni su LEAP, fare riferimento a Cisco LEAP.

D. Come funziona EAP-FAST?

R. EAP-FAST utilizza algoritmi a chiave simmetrica per ottenere un processo di autenticazione tramite tunneling. La definizione del tunnel si basa su una credenziale di accesso protetto (PAC) che EAP-FAST può fornire e gestire in modo dinamico tramite EAP-FAST tramite il server di autenticazione, autorizzazione e accounting (AAA), ad esempio Cisco Secure Access Control Server [ACS] v. 3.2.3. Con un tunnel reciprocamente autenticato, EAP-FAST offre protezione dagli attacchi dei dizionari e dalle vulnerabilità man-in-the-middle. Ecco le fasi di EAP-FAST:

EAP-FAST non solo riduce i rischi derivanti dagli attacchi dei dizionari passivi e dagli attacchi man-in-the-middle, ma consente anche un'autenticazione sicura basata sull'infrastruttura attualmente implementata.

- Fase 1: Tunnel reciprocamente autenticato: client e server AAA utilizzano la PAC per autenticarsi a vicenda e stabilire un tunnel sicuro.
- Fase 2: Esegui autenticazione client nel tunnel stabilito: il client invia nome utente e password per autenticare e stabilire i criteri di autorizzazione client.
- Facoltativamente, Fase 0: l'autenticazione EAP-FAST utilizza raramente questa fase per consentire al client di essere sottoposto a provisioning dinamico con una PAC. Questa fase genera in modo sicuro una credenziale di accesso per utente tra l'utente e la rete. La fase 1 dell'autenticazione utilizza questa credenziale per utente, nota come PAC.

Per ulteriori informazioni, fare riferimento a Cisco EAP-FAST.

D. Ci sono documenti su cisco.com che spiegano come configurare EAP in una rete WLAN Cisco?

R. Per informazioni su come configurare l'autenticazione EAP in una rete WLAN, consultare il documento sull'autenticazione EAP con il server RADIUS.

Per informazioni su come configurare l'autenticazione PEAP, consultare la nota sull'applicazione PEAP.

Per informazioni su come configurare l'autenticazione LEAP, fare riferimento a Autenticazione LEAP con un server RADIUS locale.

D. Quali sono i diversi meccanismi di crittografia più comunemente utilizzati nelle reti wireless?

R. Ecco gli schemi di crittografia più comunemente utilizzati nelle reti wireless:

- WEP
- TKIP
- AES

AES è un metodo di crittografia hardware, mentre la crittografia WEP e TKIP viene elaborata sul firmware. Con un aggiornamento del firmware, i dispositivi WEP possono supportare TKIP in modo che siano interoperabili. AES è il metodo più sicuro e veloce, mentre WEP è il meno sicuro.

D. Che cos'è la crittografia WEP?

R. WEP è l'acronimo di Wired Equivalent Privacy. Il protocollo WEP viene usato per crittografare e decrittografare i segnali dei dati che trasmettono tra dispositivi WLAN. WEP è una funzione opzionale IEEE 802.11 che impedisce la divulgazione e la modifica dei pacchetti in transito e fornisce anche il controllo dell'accesso per l'uso della rete. WEP rende un collegamento WLAN sicuro come un collegamento cablato. Come specificato dallo standard, WEP utilizza l'algoritmo RC4 con una chiave a 40 o 104 bit. RC4 è un algoritmo simmetrico perché RC4 utilizza la stessa chiave per la crittografia e la decrittografia dei dati. Quando WEP è abilitato, ogni "stazione" radio ha una chiave. La chiave viene utilizzata per codificare i dati prima della loro trasmissione attraverso le onde radio. Se una stazione riceve un pacchetto non codificato con la chiave appropriata, il pacchetto viene scartato e non viene mai consegnato all'host.

Per informazioni su come configurare WEP, fare riferimento a Configurazione di WEP (Wired Equivalent Privacy).

D. Che cos'è la rotazione dei tasti di trasmissione? Qual è la frequenza della rotazione dei tasti di trasmissione?

R. La rotazione della chiave di trasmissione consente all'access point di generare la chiave di gruppo casuale migliore possibile. La rotazione della chiave di trasmissione aggiorna periodicamente tutti i client in grado di gestire le chiavi. Quando si attiva la rotazione della chiave WEP di trasmissione, l'access point fornisce una chiave WEP di trasmissione dinamica e modifica la chiave in base all'intervallo impostato. La rotazione della chiave di trasmissione è un'eccellente alternativa a TKIP se la LAN wireless supporta dispositivi client wireless non Cisco o dispositivi che non è possibile aggiornare al firmware più recente per dispositivi client Cisco. Per informazioni

su come configurare la funzione di rotazione della chiave di trasmissione, consultare il documento sull'attivazione e disattivazione della rotazione della chiave di trasmissione.

D. Che cos'è TKIP?

R. TKIP è l'acronimo di Temporal Key Integrity Protocol. TKIP è stato introdotto per risolvere le carenze della crittografia WEP. TKIP è anche noto come hashing della chiave WEP ed è stato inizialmente chiamato WEP2. TKIP è una soluzione temporanea che risolve il problema di riutilizzo della chiave WEP. TKIP utilizza l'algoritmo RC4 per eseguire la crittografia, che è lo stesso di WEP. Una differenza importante rispetto a WEP è che TKIP cambia la chiave temporale di ogni pacchetto. La chiave temporale cambia ogni pacchetto perché il valore hash per ogni pacchetto cambia.

D. I dispositivi che utilizzano TKIP possono interagire con i dispositivi che utilizzano la crittografia WEP?

R. TKIP offre un vantaggio: le WLAN con punti di accesso e radio basati su WEP possono essere aggiornate a TKIP tramite semplici patch del firmware. Inoltre, le apparecchiature solo WEP interagiscono ancora con i dispositivi abilitati TKIP che utilizzano WEP.

D. Che cos'è il controllo dell'integrità dei messaggi (MIC)?

R. MIC è un ulteriore miglioramento per affrontare le vulnerabilità della crittografia WEP. Il MIC previene gli attacchi bit-flip sui pacchetti crittografati. Durante un attacco di tipo "bit flip", un intruso intercetta un messaggio crittografato, lo modifica e quindi ritrasmette il messaggio alterato. Il destinatario non è a conoscenza del fatto che il messaggio è danneggiato e non legittimo. Per risolvere questo problema, la funzione MIC aggiunge un campo MIC al frame wireless. Il campo MIC fornisce un controllo dell'integrità del frame che non è vulnerabile alle stesse carenze matematiche dell'ICV. Il MIC aggiunge anche un campo del numero di sequenza al frame wireless. L'access point scarta i frame ricevuti in modo non corretto.

D. Che cos'è WPA? Quali sono le differenze tra WPA 2 e WPA?

R. WPA è una soluzione di sicurezza basata su standard di Wi-Fi Alliance che risolve le vulnerabilità nelle WLAN native. WPA offre protezione avanzata dei dati e controllo dell'accesso per i sistemi WLAN. WPA risolve tutte le vulnerabilità WEP (Wired Equivalent Privacy) conosciute nell'implementazione di sicurezza IEEE 802.11 originale e offre una soluzione di sicurezza immediata per le reti WLAN in ambienti aziendali e di piccole aziende, a casa (SOHO).

WPA2 è la nuova generazione di protezione Wi-Fi. WPA2 è l'implementazione interoperabile Wi-Fi Alliance dello standard IEEE 802.11i ratificato. WPA2 implementa l'algoritmo di crittografia AES (Advanced Encryption Standard) consigliato da NIST (National Institute of Standards and Technology) con l'uso della modalità contatore con CCMP (Cipher Block Chaining Message Authentication Code Protocol). La modalità contatore AES è una cifratura a blocchi che cripta blocchi di dati a 128 bit alla volta con una chiave di cifratura a 128 bit. WPA2 offre un livello di protezione superiore rispetto a WPA. WPA2 crea nuove chiavi di sessione per ogni associazione. Le chiavi di crittografia utilizzate da WPA2 per ogni client della rete sono univoche e specifiche per tale client. In ultima analisi, ogni pacchetto inviato via etere viene crittografato con una chiave univoca.

Sia WPA1 che WPA2 possono utilizzare la crittografia TKIP o CCMP. (È vero che alcuni punti di

accesso e alcuni client limitano le combinazioni, ma ci sono quattro possibili combinazioni). La differenza tra WPA1 e WPA2 risiede negli elementi di informazione che vengono inseriti nei beacon, nelle cornici di associazione e nelle cornici handshake a 4 vie. I dati contenuti in questi elementi informativi sono sostanzialmente gli stessi, ma l'identificatore utilizzato è diverso. La differenza principale nell'handshake chiave consiste nel fatto che WPA2 include la chiave di gruppo iniziale nell'handshake a 4 vie e il primo handshake chiave di gruppo viene ignorato, mentre WPA deve eseguire questo handshake aggiuntivo per fornire le chiavi di gruppo iniziali. La reimpostazione della chiave di gruppo viene eseguita allo stesso modo. L'handshake si verifica prima della selezione e dell'utilizzo della suite di cifratura (TKIP o AES) per la trasmissione di datagrammi utente. Durante l'handshake WPA1 o WPA2, viene determinata la suite di cifratura da utilizzare. Una volta selezionata, la suite di cifratura viene utilizzata per tutto il traffico dell'utente. Pertanto, WPA1 più AES non è WPA2. WPA1 consente (ma spesso è limitato dal lato client) la cifratura TKIP o AES.

D. Che cos'è AES?

A. AES è l'acronimo di Advanced Encryption Standard. AES offre una crittografia molto più avanzata. AES utilizza l'algoritmo Rijndael, che è una cifratura a blocchi con supporto di chiavi a 128, 192 e 256 bit ed è molto più potente di RC4. Affinché i dispositivi WLAN supportino AES, l'hardware deve supportare AES anziché WEP.

D. Quali metodi di autenticazione sono supportati da un server Microsoft Internet Authentication Service (IAS)?

R. IAS supporta i seguenti protocolli di autenticazione:

- Protocollo PAP (Password Authentication Protocol)
- Protocollo SPAP (Shiva Password Authentication Protocol)
- Protocollo CHAP (Challenge Handshake Authentication Protocol)
- Protocollo MS-CHAP (Microsoft Challenge Handshake Authentication Protocol)
- Protocollo MS-CHAP v2 (Microsoft Challenge Handshake Authentication Protocol versione 2)
- CHAP (EAP-MD5 CHAP) Extensible Authentication Protocol-Message Digest 5
- EAP-Transport Layer Security (EAP-TLS)
- PEAP-MS-CHAP v2 (PEAP-MS-CHAP v2) (noto anche come PEAPv0/EAP-MSCHAPv2)

PEAP-TLS IAS in Windows 2000 Server supporta PEAP-MS-CHAP v2 e PEAP-TLS quando è installato Windows 2000 Server Service Pack 4. Per ulteriori informazioni, fare riferimento a Metodi di autenticazione da utilizzare con IAS .

D. Come viene implementata la VPN in un ambiente wireless?

A. VPN è un meccanismo di sicurezza di layer 3; al layer 2 sono implementati meccanismi di crittografia wireless. La VPN è implementata su 802.1x, EAP, WEP, TKIP e AES. Quando è presente un meccanismo di layer 2, la VPN aggiunge un sovraccarico all'implementazione. In luoghi come gli hotspot pubblici e gli hotel dove non è implementata la sicurezza, la VPN sarebbe una soluzione utile da implementare.

Domande frequenti sulla risoluzione dei problemi e la progettazione

D. Esistono best practice per installare la sicurezza wireless in una LAN wireless esterna?

R. Fare riferimento alle best practice per la sicurezza wireless esterna. In questo documento vengono fornite informazioni sulle best practice per la sicurezza relative all'installazione di una LAN wireless esterna.

D. È possibile utilizzare un server Windows 2000 o 2003 con Active Directory per un server RADIUS per autenticare i client wireless?

R. Il server Windows 2000 o 2003 con una directory attiva può funzionare come server RADIUS. Per informazioni su come configurare il server RADIUS, è necessario contattare Microsoft, poiché Cisco non supporta la configurazione del server Windows.

D. Il mio sito sta per migrare da una rete wireless aperta (serie 350 e 1200 AP) a una rete PEAP. Desidero che sia l'SSID OPEN (un SSID configurato per l'autenticazione aperta) che l'SSID PEAP (un SSID configurato per l'autenticazione PEAP) funzionino contemporaneamente sullo stesso access point. In questo modo si ha il tempo necessario per eseguire la migrazione dei client a PEAP SSID. È possibile ospitare contemporaneamente un SSID aperto e un SSID PEAP sullo stesso access point?

R. I Cisco AP supportano le VLAN (solo layer 2). Questo è in realtà l'unico modo per ottenere quello che si vuole fare. È necessario creare due VLAN, (nativa e l'altra VLAN). Quindi, è possibile avere una chiave WEP per una e nessuna chiave WEP per un'altra. In questo modo, è possibile configurare una delle VLAN per l'autenticazione aperta e l'altra VLAN per l'autenticazione PEAP. Per informazioni su come configurare le VLAN, fare riferimento a Uso delle VLAN con i dispositivi wireless Cisco Aironet.

Ènecessario configurare gli switch per il dot1Q e per il routing tra VLAN, lo switch L3 o il router.

D. Desidero configurare Cisco AP 1200 VxWorks in modo che gli utenti wireless possano autenticarsi su un concentratore VPN Cisco 3005. Quale configurazione deve essere presente sull'access point e sui client per eseguire questa operazione?

R. Non è necessaria una configurazione specifica sull'access point o sui client per questo scenario. È necessario eseguire tutte le configurazioni sul concentratore VPN.

D. Sto implementando un Cisco 1232 AG AP. Si desidera conoscere il metodo più sicuro che è possibile implementare con questo punto di accesso. Non dispongo di un server AAA e le mie uniche risorse sono l'access point e un dominio Windows 2003. Conosco bene le modalità di utilizzo delle chiavi WEP statiche a 128 bit, delle limitazioni di SSID non broadcast e di indirizzi MAC. Gli utenti utilizzano principalmente workstation Windows XP e alcuni PDA. Qual è l'implementazione più sicura per questa installazione?

R. Se non si dispone di un server RADIUS come Cisco ACS, è possibile configurare il proprio access point come server RADIUS locale per l'autenticazione LEAP, EAP-FAST o MAC.

Nota: un punto molto importante da considerare è se si desidera utilizzare i client con LEAP o EAP-FAST. In tal caso, i client devono disporre di un'utilità per supportare LEAP o EAP-FAST. L'utilità Windows XP supporta solo PEAP o EAP-TLS.

D. L'autenticazione PEAP non riesce e viene visualizzato l'errore "Autenticazione EAP-TLS o PEAP non riuscita durante l'handshake SSL". Perché?

R. Questo errore può essere dovuto all'ID bug Cisco CSCee06008 (solo utenti registrati). PEAP non funziona con ADU 1.2.0.4. Per risolvere il problema, usare la versione più recente dell'ADU.

D. È possibile disporre dell'autenticazione WPA e MAC locale sullo stesso SSID?

R. L'access point Cisco non supporta l'autenticazione MAC locale e la chiave di precondivisione ad accesso protetto Wi-Fi (WPA-PSK) nello stesso SSID (Service Set Identifier). Quando si abilita l'autenticazione MAC locale con WPA-PSK, WPA-PSK non funziona. Questo problema si verifica perché l'autenticazione MAC locale rimuove la riga della password ASCII WPA-PSK dalla configurazione.

D. Attualmente abbiamo tre Cisco 1231 Wireless AP impostati con crittografia WEP a 128 bit per la nostra VLAN dati. Il SSID non viene trasmesso. Nel nostro ambiente non è presente un server RADIUS separato. Qualcuno è riuscito a determinare la chiave WEP attraverso uno strumento di scansione, e ha usato lo strumento per un paio di settimane per monitorare il nostro traffico wireless. Come è possibile evitare questo inconveniente e rendere la rete sicura?

R. Il protocollo WEP statico è vulnerabile a questo problema e può essere derivato se un hacker cattura un numero sufficiente di pacchetti ed è in grado di ottenere due o più pacchetti con lo stesso vettore di inizializzazione (IV).

Esistono diversi modi per evitare il verificarsi di questo problema:

1. Utilizzare chiavi WEP dinamiche.
2. Utilizzare WPA.
3. Se si hanno solo schede Cisco, abilitare Per Packet Key e MIC.

D. Se si hanno due WLAN diverse, entrambe configurate per WPA (Wi-Fi Protected Access) e PSK (Pre-Shared Key), le chiavi precondivise possono essere diverse per ciascuna WLAN? Se sono diverse, influisce sull'altra WLAN configurata con una chiave precondivisa diversa?

R. La chiave WPA-PSK deve essere impostata per ciascuna rete WLAN. Se si modifica una WPA-PSK, non dovrebbe influire sull'altra WLAN configurata.

D. Nel mio ambiente uso principalmente Intel Pro/Wireless, Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) e Cisco Secure Access Control Server (ACS) 3.3 collegati ad account Windows Active Directory (AD). Il problema è che quando la password dell'utente sta per scadere, Windows non richiede all'utente di cambiare la password. Alla fine,

l'account scade. Esiste una soluzione per richiedere all'utente di modificare la password?

R. La funzione di aging delle password di Cisco Secure ACS consente di forzare gli utenti a modificare le password in una o più delle seguenti condizioni:

- Dopo un numero specificato di giorni (regole per data)
- Dopo un numero specificato di accessi (regole per utilizzo)
- Al primo accesso di un nuovo utente (regola di modifica password)

Per i dettagli su come configurare Cisco Secure ACS per questa funzione, vedere Abilitazione della durata delle password per il database utenti Cisco Secure.

D. Quando un utente accede in modalità wireless utilizzando LEAP, ottiene il proprio script di accesso per mappare le unità di rete. Tuttavia, utilizzando Wi-Fi Protected Access (WPA) o WPA2 con l'autenticazione PEAP, gli script di accesso non vengono eseguiti. Sia il client che il punto di accesso sono Cisco, come lo è RADIUS (ACS). Perché lo script di accesso non viene eseguito su RADIUS (ACS)?

R. L'autenticazione del computer è obbligatoria per il funzionamento degli script di accesso. In questo modo gli utenti wireless possono accedere alla rete per caricare gli script prima che l'utente esegua l'accesso.

Per informazioni su come configurare l'autenticazione computer con PEAP-MS-CHAPv2, fare riferimento alla configurazione di Cisco Secure ACS per Windows v3.2 con l'autenticazione computer PEAP-MS-CHAPv2.

D. In Cisco Aironet Desktop Utility (ADU) versione 3.0, quando un utente configura l'autenticazione del computer per EAP-TLS (Extensible Authentication Protocol-Transport Layer Security), ADU non consente la creazione di un profilo. Perché?

R. Ciò è dovuto all'ID bug Cisco CSCsg32032 (solo utenti registrati). Questo problema può verificarsi se nel PC client è installato il certificato del computer e non è disponibile un certificato utente.

Per risolvere il problema, copiare il certificato del computer nell'archivio utenti, creare un profilo EAP-TLS e quindi rimuovere il certificato dall'archivio utenti per la configurazione con la sola autenticazione del computer.

D. È possibile assegnare una VLAN sulla LAN wireless in base all'indirizzo MAC del client?

R. No. Non è possibile. L'assegnazione della VLAN dal server RADIUS funziona solo con l'autenticazione 802.1x, non MAC. È possibile utilizzare RADIUS per eseguire il push delle VSA con l'autenticazione MAC, se gli indirizzi MAC vengono autenticati nel server RADIUS (definito come ID utente/password in LEAP/PEAP).

Informazioni correlate

- Sicurezza della rete wireless
- White paper sulla sicurezza LAN wireless
- Panoramica della sicurezza LAN wireless
- Guida all'implementazione di EAP-TLS per le reti LAN wireless
- Cisco LEAP
- Configurazione WEP (Wired Equivalent Privacy)
- Supporto dei prodotti wireless
- Documentazione e supporto tecnico – Cisco Systems