FAQ op Cisco Aironet draadloze beveiliging

Inhoud

Inleiding

Dit document bevat informatie over de meest frequent gestelde vragen (FAQ) over Cisco Aironet draadloze beveiliging.

Algemene vragen

V. Wat is de behoefte aan draadloze beveiliging?

A. In een bekabeld netwerk blijven de gegevens in de kabels die de eindapparaten aansluiten. Maar draadloze netwerken verzenden en ontvangen gegevens via een uitzending van RF-signalen in de open lucht. Vanwege de uitgezonden aard die WLAN's gebruiken, is er een grotere bedreiging voor hackers of indringers die de gegevens kunnen benaderen of beschadigen. Om dit probleem te verminderen, vereisen alle WLAN's de toevoeging van:

1. Verificatie door gebruiker om onbevoegde toegang tot netwerkbronnen te voorkomen.
2. Gegevensbescherming ter bescherming van de integriteit en de privacy van overgedragen gegevens (ook wel codering genoemd).

Q. Wat zijn de verschillende authenticatiemethoden die de 802.11 standaard voor draadloze LAN's definieert?

A. De standaard 802.11 definieert twee mechanismen voor verificatie van draadloze LAN-clients:

1. Open-verificatie
2. Gedeeld belangrijke verificatie

Er zijn ook twee andere algemeen gebruikte mechanismen:

1. Op SSID gebaseerde verificatie
2. MAC-adresverificatie

Q. Wat is Open Verificatie?

A. Open Verificatie is in wezen een ongeldig authenticatiealgoritme, wat betekent dat er geen

verificatie van de gebruiker of machine is. Open Verificatie maakt elk apparaat mogelijk dat een verificatieaanvraag richt tot het toegangspunt (AP). Open Verificatie gebruikt duidelijke teksttransmissie om een client te laten associëren met een AP. Als geen encryptie is ingeschakeld, kan elk apparaat dat de SSID van WLAN kent, toegang tot het netwerk verkrijgen. Als Wired Equivalent Privacy (EFN) is ingeschakeld op de AP, wordt de sleutel van de EVN een middel van toegangscontrole. Een apparaat dat niet de juiste de sleutel van EFN heeft kan geen gegevens door AP verzenden zelfs als authenticatie succesvol is. En zo'n apparaat kan ook geen gegevens decrypteren die AP verstuurt.

Q. Welke stappen impliceert Open Verificatie voor een cliënt om met AP te associëren?

1. De cliënt stuurt een verzoek om onderzoek naar de AP's.
2. De AP's sturen terug sonde reacties.
3. De client evalueert de AP responsen en selecteert de beste AP.
4. De cliënt stuurt een verificatieaanvraag naar de AP.
5. AP bevestigt authenticatie en registreert de cliënt.
6. De cliënt stuurt dan een verzoek om vereniging naar de AP.
7. De AP bevestigt de vereniging en registreert de cliënt.

Q. Wat zijn de voor- en nadelen van Open Verificatie?

A. Hier zijn de voor- en nadelen van Open Verificatie:

Voordelen: Open Verificatie is een basisauthenticatiemechanisme dat u kunt gebruiken met draadloze apparaten die de complexe authenticatie algoritmen niet ondersteunen. Verificatie in de 802.11-specificatie is connectiviteit-georiënteerd. Door de vereisten voor authenticatie te ontwerpen, kunnen apparaten snel toegang krijgen tot het netwerk. In dat geval kunt u Open Verificatie gebruiken.

Nadelen: Open Verificatie biedt geen manier om te controleren of een client een geldige client is en niet een hacker-client. Als u geen EFN-encryptie met Open Verificatie gebruikt, kan elke gebruiker die de SSID van WLAN kent, het netwerk benaderen.

Q. Wat is gedeelde Key Verificatie?

A. Shared Key Verificatie werkt vergelijkbaar met Open Verificatie met één groot verschil. Wanneer u Open Verificatie met de encryptiesleutel van EFG gebruikt, wordt de sleutel van EFN gebruikt om de gegevens te versleutelen en te decrypteren, maar niet gebruikt in de authentificatiestap. In Shared Key Verificatie wordt de EFN-encryptie gebruikt voor verificatie. Net zoals Open Verificatie, vereist gedeelde Belangrijkste Verificatie dat de client en de AP de zelfde sleutel van EFN hebben. AP dat Gedeelde Belangrijkste Verificatie gebruikt verstuurt een pakket van de uitdagingstekst naar de client. De client gebruikt de lokaal geconfigureerde EFN-toets om de uitdagingstekst te versleutelen en te antwoorden met een volgende verificatieaanvraag. Als AP de authenticatieaanvraag kan decrypteren en de oorspronkelijke uitdagingtekst kan terugkrijgen, reageert AP met een authenticatiereactie die toegang tot de client verleent.

Q. Welke stappen impliceert gedeelde Belangrijkste Verificatie voor een cliënt om met AP te associëren?

1. De cliënt stuurt een verzoek om onderzoek naar de AP's.
2. De AP's sturen terug sonde reacties.
3. De client evalueert de AP responsen en selecteert de beste AP.
4. De cliënt stuurt een verificatieaanvraag naar de AP.
5. AP stuurt een authenticatiereactie die de niet gecodeerde uitdagingstekst bevat.
6. De client versleutelt de uitdagingstekst met de EFN-toets en stuurt de tekst naar de AP.
7. AP vergelijkt de niet gecodeerde uitdagingstekst met de gecodeerde uitdagingstekst. Als de authenticatie de oorspronkelijke uitdagingstekst kan decrypteren en herstellen, is de authenticatie succesvol.

Gedeelde Belangrijkste Verificatie gebruikt de encryptie van EFN tijdens het client-associatieproces.

Q. Wat zijn de voor- en nadelen van gedeelde Key Verificatie?

A. In Shared Key Verificatie wisselen de client en de AP de uitdagingtekst (duidelijke tekst) en de gecodeerde uitdaging uit. Daarom is dit type van authenticatie kwetsbaar voor mens-in-the-middle aanvallen. Een hacker kan luisteren naar de niet-gecodeerde uitdaging en de gecodeerde uitdaging, en de de sleutel van de EVN (gedeelde sleutel) uit deze informatie halen. Wanneer een hacker de sleutel van de EVN kent, wordt het hele authenticatiemechanisme gecompromitteerd en kan de hacker het WLAN-netwerk benaderen. Dit is het grootste nadeel van de gedeelde Key Verificatie.

Q. Wat is MAC-adresverificatie?

A. Hoewel de 802.11-standaard geen MAC-adresverificatie specificeert, gebruiken WLAN-netwerken deze verificatietechniek doorgaans. Vandaar dat de meeste draadloze apparaten verkopers, waaronder Cisco, MAC-adresverificatie ondersteunen.

In MAC-adresverificatie worden de klanten op basis van hun MAC-adres geauthentiseerd De MAC-adressen van de klanten worden gecontroleerd aan de hand van een lijst met MAC-adressen die lokaal op de AP of op een externe authenticatieserver zijn opgeslagen. MAC-verificatie is een sterker veiligheidsmechanisme dan de Open en Shared Key Authenticaties die 802.11 biedt. Deze vorm van authenticatie vermindert verder de kans op niet-geautoriseerde apparaten die toegang kunnen krijgen tot het netwerk.

Q. Waarom werkt MAC-verificatie niet met Wi-Fi Protected Access (WAP) in Cisco IOS-softwarerelease 12.3(8)JA2?

A. Het enige veiligheidsniveau voor MAC-verificatie is het MAC-adres van de client te controleren aan de hand van een lijst met toegestane MAC-adressen. Dit wordt als zeer zwak beschouwd. In eerdere Cisco IOS-softwarereleases kunt u MAC-verificatie en WAP configureren om de informatie te versleutelen. Maar omdat WAP zelf een MAC-adres heeft dat controleert, heeft Cisco besloten dit type configuratie niet toe te staan in latere Cisco IOS-softwarereleases en alleen om de beveiligingsfuncties te verbeteren.

Q. Kan ik SSID als methode gebruiken om draadloze apparaten te authenticeren?

A. Service Set Identifier (SSID) is een unieke, case gevoelige, alfanumerieke waarde die WLAN's als netwerknaam gebruiken. SSID is een -mechanisme dat logische scheiding van draadloze LAN's toestaat. SSID biedt geen data-privacy functies, noch SSID echt authenticeert de client aan

AP. De waarde van SSID wordt uitgezonden als duidelijke tekst in Beacons, Aanvragen van de Beeld, Beeldreacties, en andere types van kaders. Een afluisteraar kan de SSID gemakkelijk bepalen met behulp van een 802.11 draadloze LAN-pakketanalyzer, bijvoorbeeld Sniffer Pro. Cisco adviseert niet dat u SSID als een methode gebruikt om uw WLAN-netwerk te beveiligen.

Q. Als ik SSID uitzending uitzet, kan ik verbeterde veiligheid op een WLAN netwerk bereiken?

A. Wanneer u SSID uitzending uitschakelt, wordt SSID niet verstuurd in Baken-berichten. Andere kaders zoals, de Verzoeken van de Onderzoek en de Reacties van het Onderzoek hebben nog de SSID in duidelijke tekst. U bereikt geen verbeterde draadloze beveiliging als u de SSID uitschakelt. De SSID is niet ontworpen, noch bedoeld voor gebruik als beveiligingsmechanisme. Als u SSID uitzendingen uitschakelt, kunt u bovendien problemen met Wi-Fi-interoperabiliteit ondervinden voor implementaties met verschillende clients. Daarom adviseert Cisco u niet SSID als beveiligingsmodus te gebruiken.

Wat zijn de kwetsbaarheden die zijn aangetroffen in 802.11-beveiliging?

A. De belangrijkste kwetsbaarheden van de 802.11-beveiliging kunnen als volgt worden samengevat:

- Zwakke echtheidscontrole van de machine: Clientapparaten zijn echt gemaakt, geen gebruikers.
- Zwakke gegevensencryptie: Wired equivalente privacy (EVN) is ineffectief gebleken als middel om gegevens te versleutelen.
- Geen berichtintegriteit: De waarde van de integriteitscontrole (ICV) is ondoeltreffend gebleken als middel om de berichtintegriteit te waarborgen.

Q. Wat is de rol van 802.1x-verificatie in WLAN?

A. Om de tekortkomingen en de kwetsbaarheden op het gebied van beveiliging in de oorspronkelijke methoden voor echtheidscontrole aan te pakken die door de 802.11-norm worden gedefinieerd, is het 802.1X-verificatiekader opgenomen in het ontwerp voor 802.11 MAC-laagbeveiligingsverbeteringen. De IEEE 802.11-taakgroep i (TGi) ontwikkelt momenteel deze verbeteringen. Het 802.1X kader biedt de verbindingslaag met extensieve authenticatie, die normaal alleen in de hogere lagen wordt gezien.

Q. Wat zijn de drie entiteiten die het 802.1x kader definieert?

A. 802.1x-kader vereist dat deze drie logische entiteiten de apparaten op een WLAN-netwerk valideren.

1. **Leverancier**: De smeekbede bevindt zich op de draadloze LAN client en staat ook bekend als de EAP client.
2. **Authenticator**-De authenticator bevindt zich op het AP.
3. **Verificatieserver** - De authenticatieserver bevindt zich op de RADIUS-server.

Q. Hoe komt een draadloze client authenticatie voor wanneer ik het 802.1x authenticatiekader gebruik?

A. Wanneer de draadloze client (EAP client) actief wordt, authenticeert de draadloze client of met open of gedeelde authenticatie. 802.1x werkt met open authenticatie en start nadat de client succesvol verbonden is met AP. Het clientstation kan zich hiermee associëren maar kan alleen na succesvolle 802.1x-verificatie gegevensverkeer doorgeven. Hier volgen de stappen in 802.1x-verificatie:

1. AP (Authenticator) ingesteld voor 802.1x vraagt de identiteit van de gebruiker vanaf de client.
2. Clients reageren met hun identiteit binnen een vastgestelde termijn.
3. De server controleert de identiteit van de gebruiker en begint met de authenticatie met de cliënt indien de identiteit van de gebruiker in zijn database aanwezig is.
4. Server stuurt een succesbericht naar AP.
5. Zodra de client is geauthentiseerd, stuurt de server de coderingssleutel naar de AP door die wordt gebruikt om verkeer te versleutelen/decrypteren dat naar en van de client wordt verstuurd.
6. In stap 4, als de identiteit van de gebruiker niet aanwezig is in de database, druppelt de server de authenticatie af en stuurt een mislukkingsbericht naar de AP.
7. AP stuurt dit bericht naar de cliënt door, en de cliënt moet opnieuw authentiek met correcte geloofsbrieven.

Opmerking: Gedurende de 802.1x-verificatie stuurt AP de authenticatieberichten gewoon door naar en van de cliënt.

Wat zijn de verschillende MAP varianten die ik kan gebruiken met het 802.1x authenticatiekader?

A. 802.1x definieert de procedure om klanten voor authentiek te verklaren. Het MAP-type dat in het 802.1x-kader wordt gebruikt, definieert het type geloofsbrieven en de methode van authenticatie dat in de 802.1x-uitwisseling wordt gebruikt. Het 802.1x-kader kan elk van deze MAP-varianten gebruiken:

- EAP-TLS—Verlenbare verificatie-protocolbeveiliging
- EAP-FAST—EAP Flexibele verificatie via beveiligde tunnels
- EAP-SIM-EAP Subscriber-identiteitsmodule
- Cisco LEAP-Lichtgewicht-betrouwbare verificatie-protocol
- EAP-PEAP-beveiligd, duurzame verificatie-protocol
- EAP-MD5—EAP-Message Digest-algoritme 5
- EAP-OTP-EAP-een tijdwachtwoord
- EAP-TTLS-EAP-gebundelde transportlaag

Vraag. Hoe kies ik een MAP 802.1x van de verschillende beschikbare varianten?

A. De belangrijkste factor die u moet onderzoeken is of de MAP-methode al dan niet compatibel is met het bestaande netwerk. Daarnaast raadt Cisco u aan een methode te kiezen die wederzijdse authenticatie ondersteunt.

V. Wat is plaatselijke MAP-authenticatie?

A. Plaatselijke MAP is een mechanisme waarin de WLC fungeert als een authenticatieserver. Gebruikershandleidingen worden lokaal opgeslagen op de WLC om draadloze clients te authenticeren. Dit werkt als een backend-proces in afgelegen vestigingen wanneer de server uitvalt. De gebruikersreferenties kunnen worden opgehaald uit de lokale gegevensbank op de WLC of uit een externe LDAP-server. LEAP, EAP-FAST, EAP-TLS, PEAPv0/MSCHAPv2 en PEAPv1/GTC zijn verschillende MAP-authenticaties die ondersteund worden door lokale EAP.

V. Wat is Cisco LEAP?

A. Lichtgewicht Extensible Authentication Protocol (LEAP) is een eigen Cisco-methode van verificatie. Cisco LEAP is een 802.1X-verificatietype voor draadloze LAN's (WLAN's). Cisco LEAP ondersteunt sterke wederzijdse authenticatie tussen de client en een RADIUS-server via een aanmelding als gedeeld geheim. Cisco LEAP biedt dynamische coderingstoetsen per gebruiker. LEAP is de minst gecompliceerde methode om 802.1x te implementeren en vereist alleen een RADIUS-server. Raadpleeg Cisco LEAP voor informatie over LEAP.

V. Hoe werkt EAP-FAST?

A. EAP-FAST gebruikt symmetrische sleutelalgoritmen om een tunnele authenticatie te bereiken. De tunnelbouw is afhankelijk van een Protected Access Credential (PAC) dat EAP-FAST door MAP-FAST dynamisch kan worden bevoorraad en beheerd door de MAP-FAST door middel van de AAA-server (zoals de Cisco Secure Access Control Server [ACS] v.3.2.3). Met een wederzijds geauthentiseerde tunnel biedt EAP-FAST bescherming tegen woordenboekaanvallen en 'man-in-de-middenkwetsbaarheden.' Hier volgen de fasen van EAP-FAST:

EAP-FAST vermindert niet alleen de risico's van passieve woordenboekaanvallen en "man-in-de-midden"-aanvallen, maar maakt ook veilige authenticatie mogelijk op basis van de momenteel toegepaste infrastructuur.

- Fase 1: Stel wederzijds geauthentiseerde tunnel-client- en AAA-servergebruik in om PAC te authentiseren en een beveiligde tunnel op te zetten.
- Fase 2: Clientverificatie uitvoeren in de gevestigde tunnel-client verstuurt gebruikersnaam en wachtwoord om clientautorisatiebeleid voor authentiek te verklaren en vast te stellen.
- Optioneel, fase 0—EAP-FAST authenticatie gebruikt deze fase zelden om de client dynamisch van een PAC voorzien te maken. Deze fase genereert veilig een toegangsgeloof per gebruiker tussen de gebruiker en het netwerk. Fase 1 van de authenticatie gebruikt dit voor elke gebruiker bestemde gecrediteerd, de PAC.

Raadpleeg Cisco EAP-FAST voor meer informatie.

Q. Zijn er documenten op cisco.com die verklaren hoe u EAP in een Cisco WLAN-netwerk kunt configureren?

A. Raadpleeg de EAP-verificatie met RADIUS-server voor informatie over de manier waarop u de MAP-verificatie in een WLAN-netwerk kunt configureren.

Raadpleeg Protected EAP-toepassingsnota voor informatie over de manier waarop u PEAP-verificatie kunt configureren.

Raadpleeg LEAP-verificatie met een lokale RADIUS-server voor informatie over de configuratie van LEAP-verificatie.

Q. Wat zijn de verschillende coderingsmechanismen die het meest worden gebruikt in draadloze netwerken?

A. Hier worden de meest gebruikte coderingsschema's gebruikt in draadloze netwerken:

- medegebruik
- TKIP
- AES

AES is een methode voor hardwareencryptie, terwijl de encryptie van EFG en TKIP op de firmware wordt verwerkt. Met een firmware-upgrade kunnen apparaten TKIP ondersteunen zodat ze interoperabel zijn. AES is de best veilige en snelste methode, terwijl de minste veiligheid is van de verbinding met de motor.

Q. Wat is de encryptie van het gebruik van het wapen?

A. De staat van de EVN staat voor gedraaid equivalente Privacy. WLAN's worden gebruikt om gegevenssignalen te versleutelen en decrypteren die tussen WLAN-apparaten worden verzonden. De optie IEEE 802.11 is een optionele IEEE 802.11 die de bekendmaking en wijziging van pakketten in het verkeer verhindert en ook toegangscontrole voor het gebruik van het netwerk biedt. Maakt een WLAN-link zo veilig als een bekabelde link. Zoals de standaard specificeert, gebruikt EFC het RC4-algoritme met een 40-bits of 104-bits toets. RC4 is een symmetrisch algoritme omdat RC4 dezelfde sleutel voor de encryptie en de decryptie van gegevens gebruikt. Wanneer de verbinding van de radio wordt geactiveerd, heeft elk "station" een sleutel. De toets wordt gebruikt om de gegevens te vervormen voordat de gegevens via de ether worden doorgegeven. Als een station een pakket ontvangt dat niet met de juiste sleutel is bebouwd, gooit het station het pakket weg en levert nooit zo een pakket aan de host.

Raadpleeg het configureren van Wired Equivalent Privacy (EVN) voor informatie over het configureren van EFN.

Q. Wat is Broadcast Key Rotatie? Wat is de frequentie van de Broadcast Key Rotatie?

A. De omroep-sleutel kan AP de best mogelijke willekeurige groepstoets genereren. Broadcast key rotatie werkt regelmatig alle klanten bij die in staat zijn om belangrijke beheerfuncties te vervullen. Wanneer u uitzending van de sleutel de rotatie van de EVN toelaat, verstrekt AP een dynamische uitzending van de sleutel en verandert de sleutel bij het interval dat u plaatste. De omwenteling van de uitzending is een uitstekend alternatief voor TKIP als uw draadloos LAN niet-Cisco draadloze clientapparaten of apparaten ondersteunt die u niet kunt upgraden naar de nieuwste firmware voor Cisco-clientapparaten. Raadpleeg De omwenteling van de Broadcast Key Rotatie in- en uitschakelen voor informatie over de manier waarop u de omwentelingsfunctie van de uitzending kunt configureren.

V. Wat is TKIP?

A. TKIP staat voor Temporal Key Integrity Protocol. TKIP werd geïntroduceerd om de tekortkomingen in de EFG-encryptie aan te pakken. TKIP staat ook bekend als het hakken van de de sleutel van EFG en werd aanvankelijk genoemd EFG2. TKIP is een tijdelijke oplossing die het zeer belangrijke hergebruikprobleem van EFG's lost. TKIP gebruikt het RC4-algoritme om encryptie uit te voeren, wat hetzelfde is als medeweten. Een belangrijk verschil met medegebruik is dat TKIP de tijdelijke sleutel elk pakket wijzigt. De tijdelijke toets verandert elk pakje omdat de hashwaarde voor elk pakje verandert.

Q. Kunnen apparaten die TKIP gebruiken samenwerken met apparaten die de encryptie van de EVN gebruiken?

A. Een voordeel met TKIP is dat WLAN's met bestaande op EFG gebaseerde AP's en radio's naar TKIP kunnen upgraden via eenvoudige firmware-patches. Ook interopereert de apparatuur van het type van het slechts van het gebruik van de anti-TKIP nog met de apparaten die van de TKIP gebruik maken.

Q. What is Message Integrity Control (MIC)?

A. MIC is een andere verbetering om de kwetsbaarheden in de encryptie van EFG aan te pakken. MIC voorkomt bit-flip aanvallen op versleutelde pakketten. Tijdens een bit-flip-aanval, onderschept een indringer een versleuteld bericht, verandert het bericht en geeft het gewijzigde bericht vervolgens opnieuw door. De ontvanger weet niet dat de boodschap corrupt is en niet legitiem. Om dit probleem aan te pakken, voegt de MIC optie een MIC veld toe aan het draadloze kader. Het MIC-veld bevat een frame-integriteitscontrole die niet kwetsbaar is voor dezelfde wiskundige tekortkomingen als de ICV. MIC voegt ook een sequentienummer veld aan het draadloze kader toe. De AP laat beelden vallen die buiten orde ontvangen zijn.

Wat is WAP? Hoe is WAP 2 anders dan WAP?

A. WAP is een op standaarden gebaseerde beveiligingsoplossing van de Wi-Fi Alliance die de kwetsbaarheden in inheemse WLAN's aanpakt. WAP biedt verbeterde gegevensbescherming en toegangscontrole voor WLAN-systemen. WAP richt zich op alle gekende kwetsbaarheden van de Geboden Equivalent Privacy (WLAN) in de originele de veiligheidsimplementatie van IEEE 802.11 en brengt een onmiddellijke veiligheidsoplossing aan WLAN-netwerken in zowel onderneming als kleine kantoor, de omgevingen van het huiskantoor (SOHO).

WAP2 is de volgende generatie Wi-Fi-beveiliging. WAP2 is de interoperabele implementatie van de geratificeerde standaard IEEE 802.11i. WAP2 implementeert het door NIST (National Institute of Standards and Technology) aanbevolen Advanced Encryption Standard (AES)-encryptie-algoritme met het gebruik van Counter Mode met Cipher Block Chaining Message Authentication Protocol (CCMP). AES Counter Mode is een blokalgoritme die gegevens met 128 bits tegelijk versleutelt met een 128-bits coderingssleutel. WAP2 biedt een hoger beveiligingsniveau dan WAP. WAP2 maakt nieuwe sessiesleutels op elke associatie. De encryptiesleutels die WAP2 voor elke client op het netwerk gebruikt zijn uniek en specifiek voor die client. Uiteindelijk wordt elk pakje dat via de lucht wordt verstuurd, versleuteld met een unieke sleutel.

Zowel WAP1 als WAP2 kunnen TKIP of CCMP encryptie gebruiken. (Het is waar dat sommige toegangspunten en sommige klanten de combinaties beperken, maar er zijn vier mogelijke combinaties). Het verschil tussen WAP1 en WAP2 bevindt zich in de informatie die in de bakens, de associatiekaders en de 4-voudige handdruk-frames wordt geplaatst. De gegevens in deze informatie-elementen zijn in principe hetzelfde, maar de gebruikte identificator is anders. Het

belangrijkste verschil in de sleutelhanddruk is dat WAP2 de eerste groepstoets in de 4-voudige handdruk bevat en dat de eerste groepstoets wordt overgeslagen, terwijl WAP deze extra handdruk moet doen om de eerste groepstoetsen te leveren. Het opnieuw bijhouden van de groepstoets gebeurt op dezelfde manier. De handdruk komt voor de selectie en het gebruik van de algoritme reeks (TKIP of AES) voor de transmissie van gebruikerdatagrammen. Tijdens de handdruk WAP1 of WAP2 wordt de te gebruiken algoritmische reeks bepaald. Zodra deze optie is geselecteerd, wordt de ciderreeks gebruikt voor al het gebruikersverkeer. Zodoende is WAP1 plus AES niet WAP2. WAP1 staat voor (maar is vaak aan clientzijde beperkt) of het TKIP of AES-algoritme toe.

V. Wat is AES?

A. AES staat voor Advanced Encryption Standard. AES biedt een veel sterkere encryptie. AES gebruikt het Rijndael-algoritme, dat een blok-algoritme is met 128-, 192- en 256-bits ondersteuning en veel sterker is dan RC4. Voor WLAN-apparaten om AES te ondersteunen moet de hardware AES ondersteunen in plaats van Wi-Fi.

Q. Welke verificatiemethoden worden ondersteund door een server van de Microsoft Internet Accounting Service (IAS)?

A. IAS ondersteunt deze verificatieprotocollen:

- Wachtwoord-verificatieprotocol (PAP)
- Shiva Password-verificatie Protocol (SPAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
- Microsoft Challenge Handshake Authentication Protocol, versie 2 (MS-CHAP v2)
- Extensible Authentication Protocol-Message Digest 5 CHAP (EAP-MD5 CHAP)
- EAP-TLS-beveiliging (Transport Layer Security)
- Beschermde EAP-MS-CHAP v2 (PEAP-MS-CHAP v2) (ook bekend als PEAPv0/EAP-MSCHAPv2)

PEAP-TLS IAS in de Windows 2000-server ondersteunt PEAP-MS-CHAP v2 en PEAP-TLS wanneer Windows 2000 Server Service Pack 4 is geïnstalleerd. Raadpleeg voor meer informatie de verificatiemethoden voor gebruik bij de IAS .

Q. Hoe wordt VPN geïmplementeerd in een draadloze omgeving?

A. VPN is een Layer 3-beveiligingsmechanisme; Draadloze coderingsmechanismen worden geïmplementeerd op Layer 2. VPN wordt geïmplementeerd via 802.1x, EAP, EFN, TKIP en AES. Wanneer een Layer 2-mechanisme is geïnstalleerd, voegt VPN extra head toe aan de implementatie. Op plekken als publieke hotspots en hotels waar geen beveiliging is geïmplementeerd zou VPN een bruikbare oplossing zijn om uit te voeren.

FAQ voor probleemoplossing en ontwerp

V. Zijn er beste praktijken om draadloze beveiliging in een draadloos LAN in te stellen?

A. Raadpleeg de beste praktijken voor draadloze beveiliging voor buitengebruik. Dit document

bevat informatie over best practices om een draadloos LAN voor buitengebruik te implementeren.

Q. Kan ik een Windows 2000- of 2003-server met Active Directory voor een RADIUS-server gebruiken om draadloze klanten te authenticeren?

A. De Windows 2000- of 2003-server met een actieve directory kan werken als een RADIUS-server. Voor informatie over het configureren van deze RADIUS-server moet u contact opnemen met Microsoft, omdat Cisco de configuratie van de Windows-server niet ondersteunt.

Q. Mijn site staat op het punt te migreren van een open draadloos netwerk (350 en 1200 Series AP's) naar een PEAP-netwerk. Ik zou zowel de OPEN SSID (een SSID dat voor Open Verificatie wordt ingesteld) als de PEAP SSID (een SSID dat voor PEAP-verificatie is ingesteld) willen hebben om tegelijkertijd op dezelfde AP te werken. Dit geeft ons tijd om de klanten naar de PEAP SSID te migreren. Is er een manier om gelijktijdig een open SSID en een PEAP SSID op dezelfde AP te organiseren?

A. Cisco APs steunen VLANs (slechts laag 2). Dit is eigenlijk de enige manier om te bereiken wat je wilt doen. U moet twee VLAN's (native en uw andere VLAN's) maken. Dan kunt u een de sleutel van de EVN hebben voor één en geen de sleutel van de EVN voor een andere. Op deze manier kunt u één van de VLAN's voor Open Verificatie en het andere VLAN voor PEAP-verificatie configureren. Raadpleeg VLAN's gebruiken met Cisco Aironet draadloze apparatuur als u wilt begrijpen hoe u VLAN's moet configureren.

Let op dat u uw switches moet configureren voor point1Q en voor routing tussen VLAN's, uw L3-schakelaar of uw router.

Q. Ik wil mijn Cisco AP 1200 VxWorks instellen om de draadloze gebruikers te hebben authentiek aan een Cisco 3005 VPN concentrator. Welke configuratie moet er op het AP en de klanten aanwezig zijn om dit te bereiken?

A. Er is geen specifieke configuratie nodig op het AP of de klanten voor dit scenario. U moet alle configuraties op de VPN-concentrator uitvoeren.

Q. Ik implementeer een Cisco 1232AG AP. Ik zou graag de best beveiligde methode kennen die ik met deze AP kan inzetten. Ik heb geen AAA server en mijn enige middelen zijn AP en een Windows 2003 domein. Ik ben vertrouwd met hoe ik statische 128-bits-toetsen, niet-uitgezonden SSID en MAC-adresbeperkingen moet gebruiken. De gebruikers werken meestal met Windows XP-werkstations en sommige PDF-bestanden. Wat is de meest beveiligde implementatie voor deze installatie?

A. Als u geen RADIUS-server hebt zoals Cisco ACS, kunt u uw AP configureren als een lokale RADIUS-server voor LEAP, EAP-FAST of MAC-verificatie.

Opmerking: Een zeer belangrijk punt dat je moet overwegen is of je je klanten wilt gebruiken met LEAP of EAP-FAST. Als dat zo is, moeten je klanten een hulpprogramma hebben om LEAP of EAP-FAST te ondersteunen. Windows XP-toepassing ondersteunt alleen PEAP of EAP-TLS.

Q. PEAP-verificatie mislukt met de fout "EAP-TLS of PEAP-verificatie mislukt tijdens SSL-handdruk". Waarom?

A. Deze fout kan optreden door Cisco bug-ID **CSCee06008 (alleen geregistreerde klanten)**. PEAP faalt met ADU 1.2.0.4. Het resultaat voor dit probleem is om de nieuwste versie van de ADU te gebruiken.

Q. Kan ik WAP en Lokale MAC-verificatie op dezelfde SSID hebben?

A. Cisco AP ondersteunt lokale MAC-verificatie en Wi-Fi Protected Access Pre-Share Key (WAP-PSK) niet in dezelfde Service Set-Identifier (SSID). Wanneer u lokale MAC-verificatie met WAP-PSK toestaat, werkt WAP-PSK niet. Dit probleem doet zich voor omdat lokale MAC-verificatie de WAP-PSK ASCII-wachtwoordregel uit de configuratie verwijdert.

Q. Er zijn momenteel drie Cisco 1231 draadloze APs met CIERS 128-bits EFN-encryptie voor onze gegevens VLAN. We zenden de SSID niet uit. We hebben geen aparte RADIUS-server in onze omgeving. Iemand was in staat om de sleutel van de EVN te bepalen door een scangereedschap, en gebruikte het gereedschap een paar weken om ons draadloos verkeer te controleren. Hoe kunnen we dit voorkomen en het netwerk veilig maken?

A. Statische EFN is kwetsbaar voor deze kwestie, en kan afgeleid worden als een hacker genoeg pakketten opneemt en twee of meer pakketten kan verkrijgen met dezelfde initialisatie vector (IV).

Er zijn verschillende manieren om dit probleem te voorkomen:

1. Gebruik de dynamische sleutels van het EFN.
2. Gebruik WAP.
3. Als u alleen Cisco-adapters hebt, schakelt u Per Packet Key en MIC in.

Q. Als ik twee verschillende WLAN's heb, die beide zijn geconfigureerd voor Wi-Fi Protected Access (WAP)-Pre-Shared Key (PSK), kunnen de vooraf gedeelde toetsen dan anders zijn per WLAN? Als ze anders zijn, heeft dit invloed op de andere WLAN's die met een andere vooraf gedeelde sleutel zijn geconfigureerd?

A. De instelling van de WAP-PSK moet per WLAN zijn. Als u één WAP-PSK wijzigt, heeft dit geen invloed op de andere WLAN's die zijn geconfigureerd.

Q. In mijn omgeving gebruik ik vooral Intel Pro/Wireless, Extensible Authentication Protocol-Flexibele Verificatie via Secure Tunneling (EAP-FAST) en Cisco Secure Access Control Server (ACS) 3.3 gekoppeld aan Windows Active Directory (AD)-accounts. Het probleem is dat wanneer het gebruikerswachtwoord binnenkort vervalt, Windows de gebruiker niet aanzet het wachtwoord te wijzigen. Uiteindelijk verloopt de rekening. Is er een oplossing om Windows de gebruiker te vragen het wachtwoord te wijzigen?

A. Met de optie Cisco Secure ACS-wachtwoordveroudering kunt u gebruikers dwingen hun wachtwoorden te wijzigen onder een of meer van deze voorwaarden:

- Na een bepaald aantal dagen (leeftijdsgebonden regels)
- Na een bepaald aantal logins (leeftijdsafhankelijke regels)
- De eerste keer dat een nieuwe gebruiker inlogt (de regel voor het wijzigen van het wachtwoord)

Voor meer informatie over de manier waarop u Cisco Secure ACS voor deze functie kunt configureren, raadpleegt u Wachtwoord invoeren voor de Cisco Secure User Database.

Q. Wanneer een gebruiker draadloos inlogt met behulp van LEAP, krijgt hij zijn inlogscript om netwerkschijven in kaart te brengen. Met Wi-Fi Protected Access (WAP) of WAP2 met PEAP-verificatie worden de inlogscripts echter niet uitgevoerd. Zowel client- als access point zijn Cisco zoals de RADIUS (ACS). Waarom wordt het inlogscript niet uitgevoerd op de RADIUS (ACS)?

A. Machine authenticatie is verplicht voor inlogscripts die moeten werken. Dit stelt de draadloze gebruikers in staat om netwerktoegang te verkrijgen tot het laden van scripts voordat de gebruiker inlogt.

Zie Cisco Secure ACS voor Windows v3.2 configureren met PEAP-MS-CHAPv2 machineverificatie in configuratie met PEAP-MS-CHAPv2.

Q. Met ADU-release (Cisco Aironet Desktop Utility) 3.0, wanneer een gebruiker machine-verificatie vormt voor Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), stelt ADU de gebruiker niet in staat een profiel te maken. Waarom?

A. Dit komt door Cisco bug-ID CSCsg32032 (alleen geregistreerde klanten). Dit kan gebeuren als de client-pc het machinecertificaat heeft geïnstalleerd en geen gebruikerscertificaat heeft.

De tijdelijke oplossing is het machinecertificaat naar de gebruikerswinkel te kopiëren, een EAP-TLS-profiel te maken en het certificaat vervolgens uit de gebruikerswinkel te verwijderen voor de configuratie alleen van de machineverzegging.

Q. Is er een manier om VLAN op draadloos LAN toe te wijzen gebaseerd op het MAC-adres van de klant?

A. Nee. Dit is niet mogelijk. VLAN-toewijzing via RADIUS-server werkt alleen met 802.1x, geen MAC-verificatie. U kunt RADIUS gebruiken om VSA's te duwen met MAC-verificatie, als de MAC-adressen zijn geauthentiseerd op de RADIUS-server (gedefinieerd als gebruiker-id/wachtwoord in LEAP/PEAP).

Gerelateerde informatie

- Draadloze netwerkbeveiliging
- Whitepaper over draadloze LAN-beveiliging
- Overzicht van draadloze LAN-beveiliging
- EAP-TLS-implementatiegids voor draadloze LAN-netwerken
- Cisco LEAP
- Wired Equivalent Privacy (EFN) configureren

- Ondersteuning voor wireless producten
- Technische ondersteuning en documentatie – Cisco Systems