KİMLİK DOĞRULAMA VE YETKİLENDİRME

Cihazları veya kullanıcıları doğrulamaya yönelik kimlik doğrulama sürecinin yanı sıra , kullanıcının veya cihazın bağlandıktan sonra neye erişebileceğini tanımlayan yetkilendirmeler vardır. Yetkilendirme politikalarının ağ üzerinde tam olarak nasıl uygulanabileceğini detaylandırarak , segmentasyon mekanizmalarını hayata geçirebilirsiniz.

802.1X ;

IEEE 802.1X Standardı ; 802.1X İstemcisi , EAP kimlik doğrulamasına katılan bir uç noktanın parçasıdır. Eskiden bu işlevi sağlamak için yüklememiz gereken ayrı bir aracı veya yazılım parçası vardı. Artık , istemci işlevleri çoğu yaygın işletim sisteminde yerleşiktir. Diyagramlarda " isteyen " olarak etiketlenmiş uç nokta görebilirsiniz ve tamamen doğru olmasa da yeterince yakındır.

Authenticator ; 802.1X Kimlik Doğrulayıcı " Authenticator " , uç noktanın ağ bağlantısı için bağlandığı altyapı cihazıdır. Kenar anahtarı olacak kablolu uygulamalarda ve Wi-Fi'de denetleyici veya AP olacaktır. Kimlik Doğrulayıcı , EAP ile iletişim kuran uç nokta ile RADIUS protokolü ile iletişim kuran arka uç kimlik doğrulama sunucusu arasındaki bağlantıdır.

Kimlik Doğrulama Sunucusu veya AAA Sunucusu ; Kimlik Doğrulama Sunucusu , kimlik doğrulama isteğinin onaylanıp onaylanmamasına karar veren kısımdır.Genelde RADIUS sunucusudur fakat Radius gibi diğer protokoller EAP belirtimlerinde desteklenir. Kimlik Doğrulama Sunucusu amaca yönelik olabilir veya ağ erişim denetimi (NAC) ürünü gibi entegre platformun parçası olabilir. AAA , kimlik doğrulama , yetkilendirme ve muhasebe anlamına gelir. Kimlik doğrulama , kimliği doğrulama sürecidir ; yetkilendirme , erişim haklarının atanmasını içermektedir. Muhasebe sadece günlüğe kaydetmektir. 802.1X spesifikasyonunda atıfta bulunulduğunda , büyük harfle " Kimlik Doğrulama Sunucuları " görünecektir. Metnin geri kalanında , genelde kimlik doğrulama sunucularına atıfta bulunulurken , küçük harf kullanılacaktır. LAN üzerinden EAP ve EAP (EAPoL) Genişletilebilir Kimlik Doğrulama Protokolü (EAP) , IETF RFC 3748'de kimlik doğrulama çerçevesi tanımlar. LAN üzerinden EAP (EAPoL) , LAN üzerinden iletim için kapsüllenmiş EAP'nin uzantısıdır. EAP çerçevesi içinde , EAP-TLS ve EAP-MSCHAPv2 gibi belirli kimlik doğrulama türlerini öngören çok sayıda EAP yöntemi vardır. Güvenlik gereksinimleri ve kullanım durumları geliştikçe çeşitli EAP yöntemleri eklenirken , genel EAP çerçevesi tutarlı kalır.

RADIUS ; Uzaktan Kimlik Doğrulama olan Çevirmeli Kullanıcı Hizmeti (RADIUS) , kimlik doğrulama , yetkilendirme ve hesap oluşturma (AAA) için protokoldür. Günlük kullanımda RADIUS , RADIUS protokolüne veya RADIUS protokol hizmetleri sunan sunucuya atıfta bulunabilir. RADIUS protokolü , AAA için süreçleri tanımlar. Bu bağlamda , muhasebe aslında sadece aktivitenin loglanmasıdır ve temel start / stop veya daha sık ara loglama gibi farklı loglama seviyeleri vardır.

Port Varlıkları ; 802.1X'te bağlantı noktası kullanımından kaynaklanan karışıklığı gidermek için iki mantıksal Bağlantı Noktası Varlığı vardır ; yetkilendirilmiş olup olmadığına bağlı olarak uç noktaya gelen ve giden tüm paketler için kapı bekçisi görevi gören Kontrollü Bağlantı Noktası. Kimlik Doğrulayıcının (AP gibi) kimlik doğrulama (EAPoL) paketlerini uç noktadan veya istemciye , bu noktadan geçirme yolu olan Kontrolsüz Bağlantı Noktası vardır. Bunlar fiziksel bağlantı noktaları değildir. Daha soyut bir şeydir ve 802.1X'teki Kontrollü Bağlantı Noktası 802.1X zorlaması altındaki bağlantı noktası anlamına gelmez.

802.1X en sık kablosuz ağlarda kullanılsa da kablosuza özel bir protokol değildir. Orijinal standart 2001'de , 2004'te diğer ağ ortamlarını (Wi-Fi dahil) ele alan güncelleme ile ortaya çıktı. Akabinde , 2010 yılında 802.1X-REV olarak piyasaya sürülmüştür. Bunun içinde , .1X standardını desteklemek için birkaç yeni özellik eklenmiştir. Potansiyel olarak en yeni özellik , Cisco'nun TrustSec teknolojisinde kullandığı bir şey olan MACSec özelliği (802.1AE) aracılığıyla 2. katman şifrelemesiydi. MACSec ile birlikte , Güvenli Cihaz Tanımlayıcıları (DevID , 802.1AR , X.509 sertifikalarına dayalı kriptografik olarak benzersiz cihaz kimlikleri için standart) ve ağ reklamları için eklemeler ile MACSec için anahtar anlaşmalar için yeni bir standart vardı. MACSec ve onun destekleyici protokolleri , portları değiştirmek için standartlara dayalı Wi-Fi benzeri deneyim sunma bulmacasının bir parçası idi. 802.1X-REV protokollerini kullanarak , cihaz kablolu bağlantı noktasına bağlanabilir ve ağ reklamları özelliği kullanılarak Wi-Fi SSID'ler gibi çeşitli güvenlik seviyelerinde birkaç ağ ile sunulabilir. Ardından MACSec ve DevID ile güvence altına alınabilir. 2. Katmanşifreleme , ağ mimarlarına ağların güvenliğini sağlamak için güçlü ve yeni bir araç sağlayarak uç bağlantı noktalarının güvenliğini sağlama avantajlarına ek olarak kablolu trafiği şifrelemek için maliyetli güvenlik duvarlarına olan ihtiyacı ortadan kaldırır. On yıldan fazla süre sonra MACSec hala kurumsal uç anahtarlarına doğru ilerliyor. Kriptografik ilerlemeler nedeniyle , MACSec protokol paketini eklemek donanım yükseltmesidir. Çoğu kuruluşun anahtarları 15 yıllık emtia ürünü olarak gördüğü dönemde , bu yeni teknolojiyi hayata geçirmek için yeterli ivme gerçekleşmedi.

Wi-Fi Kimlik Doğrulamada Üst Düzey 802.1X İşlemi ; Wi-Fi'de 802.1X protokolü (EAP ile birlikte) , güvenli şifreleme için ilk anahtar türevleri , dağıtımları ve devam eden anahtar rotasyonları ile birlikte uç noktanın veya kullanıcının ağa kimlik doğrulamasını yönetir. Uç nokta ağa katılmayı talep ederek altyapı cihazı uç nokta ile kimlik doğrulama sürecini başlatıp akabinde kimlik doğrulama talebini yeniden paketleyip belirtilen kimlik doğrulama sunucusuna iletir. Bundan sonra ise veri yolu , sırasıyla erişim-kabul veya erişim-reddetme şeklinde gelen " evet-kimliği doğrulanmış " veya " kimliği doğrulanmamış " yanıtı ile tersine çevrilir. Kullanılan kimlik doğrulama yöntemlerine bağlı olarak , başka aracı değiş tokuşları olabilir.

Başarılı kimlik doğrulama yanıtına , dinamik VLAN ataması gibi ek yetkilendirme bilgileri de eşlik edebilir. Kimlik doğrulama sırasında , Wi-Fi altyapısı uç nokta ile iletişim kurmak için EAPoL protokolünü kullanarak bunları RADIUS / AAA sunucusuna göndermek için RADIUS protokol paketleri olarak yeniden paketleyecektir.

Altyapı cihazları (kablosuz denetleyiciler veya AP'ler gibi) , istek ve yanıtın yeniden paketlenmesi ve iletilmesi , daha sonra anahtar yönetimi dışında kimlik doğrulama sürecine katılmazlar. Bu , tüm kimlik doğrulama parametrelerinin (EAP yöntemleri dahil) müzakeresinin sadece uç noktayı ve kimlik doğrulama sunucusunu içerdiği anlamına gelir. Altyapı cihazı sadece bir aracıdır. WPA3-Enterprise'ın belirli uygulamalarıyla (özellikle EAP-TLS kullanan) , Wi-Fi altyapısı sunucu sertifikasının doğrulanmasında rol oynayacaktır. Kimlik doğrulama sırasında altyapıya (802.1X Kimlik Doğrulayıcı) biraz daha fazla rol veren yeni bir işlevdir. 802.1X kullanırken , ister kablolu ister kablosuz bağlantı noktasında olsun , uç noktanın kimliği doğrulanana kadar bağlantı noktası kapalı kabul edilir. Bu süre boyunca , uç noktaya girip çıkmasına izin verilen paketler sadece kimlik doğrulama için EAP paketleridir. 802.1X'i sıkı bir kapı olarak düşünün , hiçbir şey geçmiyor. Bu bağlantı noktası başarılı kimlik doğrulama ile açılana kadar ping işlemi , DHCP isteği veya hiçbir şey yoktur. İki (fiziksel olmayan) 802.1X bağlantı noktası öğesinin işlevinde açıklanmıştır ; Kontrol Edilmeyen Bağlantı Noktası , uç noktanın kimlik doğrulaması yapabilmesi için EAP trafiğini geçirerek Kontrollü Bağlantı Noktası işlevi , diğer paketleri uç noktaya veya uç noktadan engelleyen ağ geçidi bekçisi olarak hizmet eder. 802.1X , 2. katmanda çalışır. DHCP kullanan uç noktaların 802.1X/EAP işlemleri sırasında IP adresi bile olmaz. Wi-Fi ürünleri ile güvenlik ve ağ izleme araçlarının bu süreç boyunca uç noktaya ilişkin görünürlüğe sahip değildir. Görünürlük eksikliği 802.1X sorun gidermeyi daha zor hale getirmektedir.

Satıcıya Özel Niteliklere Örnekler ;

Cisco, Cisco-AVP (Öznitelik) , CiscoSecure-Defined-ACL; value=guest_acl (Örnek Değer) , İndirilebilir ACL gönderir RADIUS'tan WLC'ye (Açıklama).

Aruba Networks (Satıcı) , Aruba-AVP (Öznitelik) , Aruba-Kullanıcı Rolü (Örnek Değer) , Adlandırılmış bir role dayalı erişim kontrolünü zorlamak için RADIUS'tan Aruba Wi-Fi'ye talimatlar gönderir (Açıklama).

Aruba Networks (Satıcı) , Aruba-AVP (Öznitelik) , Aruba-Location-ID (Örnek Değer) , AP adını tanımlamak için Aruba'dan RADIUS'a gönderildi (Açıklama).

RADIUS Sunucuları , RADIUS Öznitelikleri ve VSA ; RADIUS , hem bir protokoldür (IETF RFC 2865) hem de RADIUS hizmetlerini sağlayan kimlik doğrulama sunucusunun ortak adıdır. RADIUS sunucuları ve protokolleri için çok daha fazlası bulunmaktadır fakat Wi-Fi ve LAN tabanlı ağ kimlik doğrulaması amacıyla aşina olunması gereken sadece birkaç ilgili kısım vardır. Ek A , " 802.1X'i Microsoft NPS ile Yapılandırmaya İlişkin Notlar " da , Microsoft NPS'de RADIUS kurulumuna ilişkin ipuçları içeren nasıl yapılır kılavuzu bulabilirsiniz. RADIUS sunucusu , AAA sunucusudur ve 802.1X ve EAP spesifikasyonlarında kimlik doğrulama sunucusu olarak anılır.

RADIUS Sunucuları ; RADIUS sunucuları AAA hizmetleri sağlar ; kimlik doğrulama , yetkilendirme (erişim hakları) , hesap oluşturma (günlüğe kaydetme). RADIUS sunucusu , altyapı cihazlarından (anahtarlar , AP , denetleyiciler vb.) gelen kimlik doğrulama isteklerini işleyen , amaca yönelik olarak oluşturulmuş sunucu veya hizmettir. RADIUS sunucuları , ağ kaynaklarına erişim amacıyla (802.1X güvenli SSID'de olduğu gibi) kullanıcıların kimliğini doğrulayarak ağ cihazlarının yönetimi için kullanıcıların kimliğini doğrulayabilir (TACACS+'ya benzer fakat aynı kontrol ayrıntı düzeyi olmadan). RADIUS sunucusu , genelde SSL-VPN ve cihaz yönetimi gibi altyapının diğer bölümlerinden gelen kimlik doğrulama isteklerine hizmet edecektir. Kimlik doğrulama (RADIUS) sunucusu çoğunlukla , kullanıcı gruplarının ve kimlik bilgilerine sahip kullanıcı hesaplarının depolandığı dizin hizmetine (Microsoft Active Directory gibi) bağlanır. RADIUS sunucularında yerel kullanıcı hesapları oluşturmak mümkündür fakat etki alanı kullanıcı hesapları her zaman bir dizinde olacaktır. RADIUS sunucularındaki yerel kullanıcı hesapları , çoğunlukla kullanıcıların veya cihazların kurumsal etki alanı dizininde bulunmasının istenmediği belirli BYOD ve konuk kaydı kullanım durumları gibi etki alanı olmayan hesapların hizmetindedir.

RADIUS Sunucuları ve NAC Ürünleri ; RADIUS hizmetleri sunan ürünler arasında Microsoft Server Network Policy Server (NPS) , Cisco Identity Services Engine (ISE) , Aruba ClearPass Policy Manager , Fortinet FortiAuthenticator , FreeRADIUS , Pulse Secure Steel-Belted RADIUS yer almaktadır. RADIUS etkin ürünlerin birçoğunun NAC çözümlerine girmektedir. NAC ürünleri ile RADIUS sunucuları arasındaki çizgi bulanıktır çünkü birçok profesyonel NAC'nin duruş ve profil oluşturma anlamına geldiğini düşünürken , pratikte birçok kuruluş NAC ürünlerini ek işlevler için değil , sadece kimlik doğrulama özellikleri için kullanır. Kuruluşların Cisco ISE veya Aruba ClearPass gibi araçlara sahip olması , bunları sadece RADIUS veya TACACS+ hizmetleri için kullanması son derece yaygındır. Bu durumlarda , ISE veya ClearPass , mimarideki basitçe RADIUS sunucusu veya kimlik doğrulama sunucusudur.

802.1X , işlem için sadece standart RADIUS protokol desteğini gerektirse de , NAC ürünleri , kimlik doğrulama ve yetkilendirme için daha ayrıntılı politika denetimi dahil olmak üzere ek özellik setleri ekler. Microsoft NPS'nin doğal olarak mantık VE değerlendirme ilkeleri oluşturmak için basit seçenek sunmamasıdır. Kimlik doğrulaması yapmak için kullanıcının ve cihazın hem yetkilendirilmiş hem de bellekte olması gerektiğini söyleyen tek bir ilke oluşturamazsınız. İşlem son derece sınırlayıcıdır ve çalışanların etki alanı kimlik bilgileriyle (MSCHAPv2 ile EAP-PEAP ile) kişisel cihazları kullanmalarının kısıtlanamamasıyla sonuçlanır. Diğer ürünlerin çoğu , iç içe mantık işlevleriyle (VE ve VEYA deyimlerini hiyerarşide birleştirmek) son derece karmaşık ve ayrıntılı politikalara izin verir. Ayrıca profil oluşturma (cihaz türünü tanımlama) ve duruş oluşturma (uç noktayı kontrol etme) gibi ek politika girdileri sağlar. NAC ürünleri , RADIUS ve EAP'nin temel evet / hayır işlemlerinin ötesinde bir dizi özellik sunar. Yaygın kullanım durumları ve özellikleri şöyledir ; Parçacıklı ilkeler için AND ve OR gibi mantıksal ifadeleri katmanlama ve iç içe yerleştirme yeteneği. Uç nokta güvenlik duruşunu yetkilendirme kararlarına dahil etme seçenekleri. Kayıt , karantina ve düzeltme dahil ağ sınıflarına dinamik atama desteği. Kullanıcı yetkilendirmesi , cihaz duruşu , konum ve bağlantı türü gibi çeşitli girdilere dayalı politika kararlarını uygulama konusunda gelişmiş yetenek. Mobil cihaz yönetimi (MDM) araçları dahil olmak üzere yönetim için üçüncü taraf entegrasyonları için destek eklenmiştir. Güvenlik bilgileri ve olay yönetimi (SIEM) araçları gibi güvenlik otomasyonu için üçüncü taraf entegrasyonları için destek eklenmiştir.

Bazı satıcılar , belirli NAC benzeri işlevleri artırmak için Wi-Fi ürünlerine kendi gizli özelliklerini ekler. Aruba ürünlerinin çoğu sürümü , harici NAC ürünü veya gelişmiş kimlik doğrulama sunucusu olmadan hem kullanıcı hem de makine kimlik doğrulamasını destekler. Ek denetleyici özellik lisansları gerekebilir (Aruba'nın durumunda Politika Yürütme Güvenlik Duvarı veya PEF gibi). Ortamınız ister Aruba ister başka bir ürün kullanıyor olsun , satıcı hesap ekibinize veya ürün belgelerine danışınız i kullanıcı ve makine kimlik doğrulaması seçeneği olup olmadığına bakınız ; bu , hemen hemen her mimarinin parçası olması gereken güvenlik özelliğidir.

RADIUS , EAP ve Altyapı Cihazlarının İlişkisi ; 802.1X kimlik doğrulama işleminde EAP ile ilgili her şey uç nokta ve kimlik doğrulama (RADIUS) sunucusu arasında görüşülse de , RADIUS protokol paketleri altyapı aygıtı (AP veya denetleyici gibi) ile RADIUS sunucusu arasında geçirilir. Altyapı cihazı ile uç nokta arasında kullanılan protokol EAPoL'dur (LAN üzerinden EAP). EAP paketlerini kimlik doğrulama için alan ve kimlik doğrulama sunucusuyla iletişim kurmak için bunları RADIUS olarak saran veya yeniden paketleyen altyapı cihazıdır (802.1X Kimlik Doğrulayıcı). 802.1X'teki en temel işleminde RADIUS , EAP kimlik doğrulama çerçevesini kolaylaştıran ve ağa katılmaya çalışan uç nokta için erişim kabul-kimliği doğrulandı veya erişim reddetme-kimliği doğrulanmadı yanıtı döndüren protokoldür. Wi-Fi'de , kimlik doğrulama sunucusu (çoğunlukla RADIUS sunucusu) , 802.1X için aşağıdakiler de dahil olmak üzere birkaç kritik işlevi yerine getirir ; Ağ için kullanılabilen EAP yöntemlerini tanımlama. Uç noktanın kimliğini doğrulama. İkili ana anahtarı (PMK) oluşturma ve 802.1X Kimlik Doğrulayıcıya (Wi-Fi AP'ler veya denetleyici) teslim etme. Boşta kalma zamanlayıcısını ayarlama. Yeniden kimlik doğrulama için oturum zamanlayıcısını belirleme.

Kimlik doğrulama için zamanlayıcı ayarları sistemin düzgün çalışması için kritik öneme sahiptir ve mimariye bağlı olarak varsayılandan ayarlamalar gerektirebilir. Altyapı , oturumun süresini belirlemek için Session-Timeout özniteliğinin değerini ve oturumun zamanlayıcısı sona erdiğinde cihaz eylemini belirlemek için Termination-Action özniteliğinin değerini kullanır. Termination-Action özniteliği mevcutsa ve değeri RADIUS-Request ise altyapı uç noktayı yeniden doğrular. Termination-Action özniteliği mevcut değilse veya değeri Varsayılan ise altyapı oturumu sonlandırır.

RADIUS Nitelikleri ; RADIUS öznitelikleri , RADIUS kimlik doğrulamasında yer alan ayrı öğelerdir ve IETF RFC'lerinde tanımlanan yaklaşık 255 standart RADIUS özniteliği vardır. Marka , model veya versiyondan bağımsız olarak herhangi bir altyapı ekipmanı tarafından anlaşılmalıdır ve bunlara uyulmalıdır.

Ortak RADIUS Nitelikleri ; Kullanıcı için öznitelikler , kimlik bilgisi sorgulama bileşenleri (EAP yöntemleri gibi) , talep eden altyapı (kontrolör IP adresi ve SSID gibi) , oturum bilgileri (zaman aşımları ve günlük kaydı gibi) ve yetkilendirme talimatları için döndürülen özniteliklerdir. RADIUS öznitelikleri , standart RADIUS öznitelikleri veya genişletilmiş RADIUS öznitelikleri biçiminde olabilir. NAS Bağlantı Noktası Türü'nün 61 öznitelik değeri , 19 değerinde , bunun 802.11 WLAN ortamı olduğu anlamına gelir. Yüzlerce nitelik vardır ; Wi-Fi kimlik doğrulamasında ve yetkilendirmede kullanılan birkaç ortak özelliğin bir örneğini, temaya göre rahat şekilde gruplandırılmış olarak göstermektedir. Sezgisel olmayabilecek birkaç tanesine işaret etmek gerekirse , RADIUS " NAS " , 802.1X Kimlik Doğrulayıcı olarak görev yapan altyapı cihazı olan Ağ Erişim Sunucusu'dur.

NAS-IP-Adresi ; Kimlik doğrulama isteğini gönderen altyapı cihazının (AP veya denetleyici) IP adresidir. Bu genelde Wi-Fi cihazlarında yapılandırılabilir.

NAS Bağlantı Noktası ; Kablolu 802.1X dağıtımlarında daha kullanışlıdır ve Wi-Fi günlüklerinde görünebilir veya görünmeyebilir. 16 bitlik bir ilişki kimliği içerebilir.

NAS-Port-Tipi ; Orta türü tanımlar ; bu durumda tip 19 " Kablosuz - IEEE 802.11 " dir.

Aranan İstasyon Kimliği ; Uç noktanın kimlik doğrulaması yaptığı AP'nin MAC adresi , SSID ile eklenir.

Çağrı İstasyonu Kimliği ; Kimlik doğrulaması yapmaya çalışan uç noktanın MAC adresidir.

Wi-Fi'de standart RADIUS özniteliklerinin örneklerini görmek için bu web sitesini ziyaret edebilirsiniz.

Başarılı kimlik doğrulaması varsayarsak , RADIUS sunucusu , cihazın yetkilendirilmesiyle ilgili belirli RADIUS özniteliklerini döndürebilir. Neye erişmesine izin verildiğini tanımlar. RADIUS protokolü , eski arama hizmetlerinden operatör işlemlerine kadar birçok amaç için kullanılır. Bu nedenle tümü Wi-Fi ağ kimlik doğrulaması için kullanılmaz.

Dinamik VLAN'lar için RADIUS Nitelikleri ; Wi-Fi'de döndürülen özel RADIUS özniteliğinin en yaygın kullanımı , dinamik VLAN atamasıdır. Dinamik VLAN atamaları ile SSID'ye bağlı statik VLAN yerine , altyapıya RADIUS sunucusundan dinamik VLAN kabul etmesi söylenebilir. RADIUS ilkesi , herhangi bir sayıda özelliğe dayalı olarak bir cihaz veya kullanıcı için bir VLAN'ı eşleyebilir veya önerebilir. Genelde grup üyeliği tarafından tanımlanan bir kullanıcı rolüne eklenir. NAC ürünleriyle yapılan uygulamalar , düzeltme veya karantina için belirlenmiş bir ağa bir uç noktayı gönderme dahil olmak üzere dinamik VLAN ataması için genişletilmiş kullanım durumlarına sahip olabilir.

Dinamik VLAN ataması için standart RADIUS öznitelikleri ve değerleri ;

ÖZELLİK	AÇIKLAMA	VERİ TİPİ ,	ÖRNEK DETAYLAR
81	Tunnel-Private-Group-ID	text	VLAN kimliğinin metin değeri
64	Tunnel-Type	enum	Value " Değer " 13 = VLAN
6	Service-Type	enum	Value " Değer " 2 = Framed
65	Tunnel-Medium-Type	enum	Value " Değer " 6 = 802 (kablolu yada Wi-Fi)

Standart Radius Özellikleri ; Cisco , Aruba Networks , Juniper gibi kurumsal düzeydeki çözümlerin çoğu , dinamik VLAN atamaları için bunlar gibi nitelikleri sürekli olarak kullanmıştır. Çoğunlukla RADIUS kimlik doğrulamalarınız düzgün çalışmıyorsa veya hiç çalışmıyorsa satıcı desteğinin değişiklik göstermesi ve desteklenmeyen bir şey deniyor olmanız olabilir.

RADIUS Satıcıya Özel Nitelikler ; Döndürülen ek nitelikler , ürüne özel talimatlar gönderen özel Satıcıya Özel Nitelikler (VSA) da içerebilir. Cisco WLC'ye bu kullanıcıya indirilebilir erişim kontrol listesi (ACL) uygulamasını söyleme veya Aruba'ya talimat veren Aruba rol özniteliği döndürmek için denetleyici olabilir. Bazı kimlik doğrulama sunucuları önceden yüklenmiş VSA paketi ile gelebilirken , diğerleri kutudan çıktığı gibi yalnızca standart RADIUS özniteliklerini sunar. Her iki durumda da , VSA'lara ihtiyaç duyulursa , ek işlevsellik için bir sözlük dosyası olarak RADIUS sunucusuna kolayca aktarılabilirler. Wi-Fi'de kullanılan VSA'lar genelde yetkilendirme ve erişim kontrolü ile ilgilidir. İndirilebilir ACL veya kablosuz altyapı içinde satıcı tarafından belirlenen bir role veya güvenlik profiline eşleme şeklinde gelebilir.

Standart RADIUS öznitelikleri , kurumsal kullanım durumlarında gereken özelliklerin çoğunu sunar. Görev , standart RADIUS öznitelikleri ile gerçekleştirilebiliyorsa , VSA'lar yerine bunları kullanmanız önerilir. Mimariniz VSA'ları gerektiriyorsa , yetkilendirme ve erişim kontrollerinin tasarlandığı gibi çalıştığından emin olmak için daha düzenli testler eklemeniz önemle tavsiye edilir. VSA'larınız dinamik ACL'leri zorunlu kılıyorsa , politikanın düzgün şekilde uygulanmadığı durumlarda uyarı verecek izleme çözümüne sahip olunuz.

RADIUS Politikaları ; RADIUS ilkeleri , ilkenin ne zaman kullanılacağını , izin verilen kimlik doğrulama yöntemlerini , başarılı kimlik doğrulamayla birlikte döndürülecek tüm yetkilendirme parametrelerini değerlendirmek için koşulları tanımlar. Her RADIUS sunucusu markası , bir ilkenin bileşenleri için kendi etiketlerine sahip olacaktır fakat hepsi aynı temel yapıya sahiptir. Microsoft NPS ağ ilkesinin üç öğesidir.

Koşullar ; Politikanın uygulanabilmesi için gelen isteğin belirtilen koşullarla eşleşmesi gerekir. Koşullar , tüm gelen Wi-Fi istekleri için herhangi bir / tüm işlemeyi veya belirli denetleyicilerden gelen isteklerle eşleştirmeyi (NAS IPv4 adresi özniteliğini kullanarak) , belirli konumlardan gelen istekleri , belirli bir kullanıcı , bilgisayar grubuna üyeliği içerebilir. Çoğu RADIUS sunucusu , eski güvenlik duvarı kuralı değerlendirmesine benzer şekilde , ölçütlerle eşleşen ilk ilkeyi kullanarak yukarıdan aşağıya biçimde etkin / etkinleştirilmiş ilkeler listesine göre değerlendirme yapar.

Kısıtlamalar ; İlke kısıtlamaları , izin verilen kimlik doğrulama türleri (EAP yöntemleri ve iç kimlik doğrulama yöntemleri) , oturum zaman aşımları , gün ve saat kısıtlamaları gibi parametreleri tanımlar. RADIUS'un etkin olduğu NAC ürünlerinde bunlar ; bir uç noktanın ne olduğunu ve mevcut güvenlik durumunu dikkate alan profil oluşturma veya duruş kriterlerini de içerebilir.

Ayarlar ; Ayarlar alanında , erişim-kabul (başarılı kimlik doğrulama) ile döndürülecek RADIUS öznitelikleri uygulanır. Dinamik VLAN atamasını veya standart , satıcıya özel RADIUS özniteliklerini kullanan diğer parametreleri içerebilir.

Radius , Radsec , Diameter ; RADIUS protokolü 1990'lardan beri var ve anlaşılır şekilde , özellikle güvenlik özellikleriyle ilgili çeşitli eksiklikleri bulunmaktadır. O zamandan beri , uygun şekilde Diameter adında yeni AAA protokolü ortaya çıkmıştır. Diameter , AAA'yı bağlantı yönelimli bir protokole (özellikle UPD'den TCP'ye geçiş) yükselterek ve şifreleme ekleyerek RADIUS'taki güvenlik açıklarını çözmek için tasarlanmıştır. Daha güvenilir ve güvenli AAA protokolüne sahip Diameter yaygın olarak benimsenmiyor ve kurumsal ortamlarda neredeyse yoktur. Diameter , çeşitli ek özelliklerle RADIUS'a benzer şekilde çalışır. Bu nedenle burada elde ettiğiniz RADIUS hızlı başlangıcı , Diameterin temel AAA kavramlarına dönüşecektir. Bu arada , TLS veya DTLS üzerinden TCP kullanan RADIUS olan RADSEC vardır. Yani , Diameter'ın söz verdiği gibi , bağlantı odaklı protokol ve şifreleme elde ederiz.

RADIUS Sunucuları , İstemciler ve Paylaşılan Sırlar ; RADIUS istemcileri (802.1X Kimlik Doğrulayıcıları) , uç noktalar adına RADIUS sunucusuna (802.1X kimlik doğrulama sunucusu) kimlik doğrulama istekleri gönderecek olan altyapı bileşenleridir. Çoğu ortamda , kablosuz denetleyiciler , APler veya kablosuz ağ geçidi cihazları , kablolu ve uzaktan erişim talepleri için anahtarlar , güvenlik duvarları veya diğer ağ cihazları olacaktır. RADIUS istemcilerini yapılandırdığınızda , sadece kimlik doğrulama isteğinde bulunmak için izin verilenlerin izin verilenler listesidir.

RADIUS İstemcilerini Belirtme ; Tüm ürünlerde , RADIUS istemcileri , host bilgisayar IP adresleri , FQDN veya alt ağ ile tanımlanan ağlar dahil olmak üzere birkaç yolla belirtilebilir. Her RADIUS istemci girişi (IP veya ağ üzerinden) , RADIUS paylaşılan sırrını belirtir. İzin verilen istek sahibi olarak RADIUS sunucusunda kimliğini doğrulamak için altyapı aygıtı tarafından kullanılan paroladır. Kimlik doğrulama sunucuları birçok RADIUS istemcisini destekler. Bu nedenle tek bir tümünü yakalama veya joker karakter girişi yapılandırmanıza gerek yoktur. Bunun yerine , RADIUS istemcilerini , çevreye ve ağ yönetimi segmentasyonunun derecesine göre makul olduğu kadar spesifik olacak şekilde planlayınız. Burada gerekli olan , büyük ölçüde Wi-Fi altyapısının nasıl yapılandırıldığına bağlı olacaktır ; RADIUS istekleri , kablosuz denetleyici veya ağ geçidi aygıtı gibi merkezi bir kaynaktan gelebilir veya her bir AP'den veya sanal davranan belirlenmiş AP'den gelebilir. Wi-Fi altyapısında bu ayarlar her ürünün uygulamasına özeldir ve sıklıkla yapılandırılabilir. Birçok Wi-Fi ürününde , RADIUS istemci kaynak IP'si olarak sabit (gerçek veya sanal) IP adresi belirleme seçeneğiniz vardır. NAS IP'nin RADIUS özniteliği , Ağ Erişim Sunucusu IP adresi , RADIUS terimleriyle eşlenir. Bireysel AP'lerin RADIUS istekleri gönderdiği bulut tarafından yönetilen bir mimaride , AP yönetim VLAN'ınız varsa , bu ağı onaylı RADIUS istemci ağı olarak ekleyebilirsiniz. Denetleyicisiz ve bulutsuz yerel küme AP mimarisi için kümenin paylaşılan veya sanal IP'sini RADIUS istemci kaynağı olarak belirtmeyi tercih edebilirsiniz. Bu durumda bu IP'yi RADIUS istemcisi olarak girersiniz. RADIUS sunucusu , yetkisiz RADIUS istemcisinden istek alırsa , bu olayı günlüğe kaydeder ve sorun gidermede sizin için kullanılabilir (günlüğe kaydetmenin etkin olduğu varsayılarak).

RADIUS Paylaşılan Sırları ; Bazı ürünler (Microsoft NPS gibi) oluşturulduktan sonra paylaşılan sırrı görüntülemenize izin vermeyeceğinden , yapılandırdığınız tüm RADIUS istemcileri için paylaşılan sırları güvenli bir yere (parola kasası gibi) kaydettiğinizden emin olun. Sunucu oluşturulduktan sonra paylaşılan sırrı görmenize izin vermeyebilirken , birçok Wi-Fi ürünü onu CLI veya GUI'de görüntülemenize izin verecektir. RADIUS sunucusunun yanı sıra altyapı cihazında (802.1X Kimlik Doğrulayıcılar) paylaşılan sırrı girmeniz gerekecek , aksi takdirde RADIUS sunucusu , bu RADIUS istemcilerinden gelen tüm kimlik doğrulama isteklerini reddedecektir.

Radius Güvenliği ; RADIUS hizmetleri , güvenilir ağlarda konuşlandırılmak üzere tasarlanmıştır ve bu nedenle , paylaşılan sır dahil olmak üzere verileri şifrelemez yani ağ üzerinden düz metin olarak gönderilir. Bu nedenle , başka hiçbir şey için gerçek parola olan paylaşılan bir sır asla belirtmemelisiniz. Şifreleme ve gizlilik eksikliği nedeniyle , TLS (RADSEC) üzerinden RADIUS'un yeni uygulamaları daha popüler hale gelmektedir. RADSEC on yılı aşkın bir süredir kullanılmaktadır fakat muhtemelen Microsoft'un IAS ve NPS gibi birçok popüler ürününde yerel olarak desteklenmediği için kuruluşlarda bu kadar yaygın olarak benimsenmemiştir. RADSEC en yaygın olarak , güvenilmeyen ağlarda kimlik doğrulaması için veya farklı tür veya sahiplik ağları (hücreselden Wi-Fi'ye kadar) arasında dolaşımdayken ağ yönetimi kimlik doğrulaması için kullanılır. RADSEC kullanan en büyük dağıtımlardan biri de Amerika Birleşik Devletleri'ndeki üniversiteler arasında popüler olan Eduroam hizmetidir. Cisco ISE , Aruba ClearPass Policy Manager ve Fortinet FortiAuthenticator gibi daha güçlü RADIUS özellikli ürünler RADSEC'i destekler.

Diğer gereklilikler ; İlkelere ve RADIUS istemcilerine ek olarak , RADIUS sunucuları , altyapıyla çalışmak için bazı ek girdiler ve entegrasyonlar gerektirir. Özellikle , kimlik doğrulama dizinine bağlantı, günlüğe kaydetme (muhasebe) ve sertifikalardır.

Kullanıcı Dizinleri ; Özellikleri temel RADIUS işlevlerinin ötesine taşıyan NAC ürünlerinin yanı sıra , kullanıcı ve cihaz deposu genelde RADIUS sunucusunun dışındadır. RADIUS'tan en yaygın bağlantı , Microsoft Active Directory veya benzeri LDAP'ye olacaktır. RADIUS sunucusundan bağımsız olarak , bir veya daha fazla kimlik doğrulama kaynağına bağlantı gerekli olacaktır. NAC ürünleri için konuk ve BYOD yönetimi amacıyla kullanıcı veya cihaz kaydı için dahili bir veritabanı olabilir.

Sunucu Sertifikası ; Uç noktanın nasıl doğrulandığına bakılmaksızın (kullanıcı adı / parola veya sertifika) , sunucunun her zaman bir sertifika ile kimliğini doğrulayacağıdır. Bu , 802.1X'in karşılıklı kimlik doğrulama ilkesinin temelidir.

Kayıt / Muhasebe ; " AAA "daki üçüncü "A" muhasebedir yani sadece günlüğe kaydetme anlamına gelir. Microsoft NPS gibi bazı RADIUS ürünlerinde günlük kaydı yapılandırılmalıdır (yerel bir metin dosyasına veya SQL veritabanına).

RADIUS Muhasebesi Üzerine Ek Notlar ; RADIUS hesabının (günlük kaydının) uygun şekilde etkinleştirilmesi , hem denetim amaçları hem de sorun giderme için güvenliğin kritik bir parçasıdır. Günlüğe kaydetme yalnızca etkinleştirilebilir ve yapılmalıdır , aynı zamanda SIEM araçları da dahil olmak üzere izleme için güvenlik araçlarına veri göndermek üzere yapılandırılabilir ve olmalıdır. RADIUS hizmetlerine sahip birçok NAC ürününün kendi günlük kaydı varsayılan olarak etkinleştirilecektir. Ancak , Microsoft NPS kullanıyorsanız , günlüğe kaydetmeyi manuel olarak yapılandırmanız gerekir. NPS ile günlüğe kaydetmeyi etkinleştirmeniz ve yerel metin dosyasında mı yoksa SQL veritabanında mı oturum açacağınızı seçmeniz gerekir. Günlüğe kaydetme düzeyini (aralıklı günlüğe kaydetmeye karşı başlatma / durdurma , yetkilendirme değişiklikleri) ve günlüğe kaydetme hedefi mevcut değilse sunucunun ne yapması gerektiğini yapılandıracaksınız.

Çoğu dağıtım için muhasebe ve kimlik doğrulama isteklerinin günlüğe kaydedilmesi ve periyodik durum günlüğünün atlanması önerilir. Günlüğe kaydetme kullanılamıyorsa ne yapılacağını belirleme seçeneği de vardır ; " Kimlik doğrulamaya izin verin veya bunları atınız " Bu ayar , kuruluşun güvenlik gereksinimlerine göre uygulanmalıdır. Güvenlik bilincine sahip ve düzenlemeye tabi endüstriler için kaydetme hatası atma seçilmelidir.

Yetki Değişikliği ve Bağlantıyı Kes Mesajları ; Standart RADIUS işlemi kapsamında , sunucu uç noktanın kimlik doğrulama isteğini kabul eder veya reddeder. Başarılı kimlik doğrulama ile birlikte ek parametreler (dinamik VLAN gibi) geri gönderebilir fakat kullanıcı veya cihazın kimliği RADIUS ile doğrulandıktan sonra yeniden bağlanana veya altyapı yeniden kimlik doğrulamayı zorlayana kadar devam etmek iyidir. Bu modelde desteklenmeyen şey ise kimlik doğrulama altyapısının bir uç noktanın yetkilendirme durumunu kaldırmak veya değiştirmek istediği senaryoları işlemenin bir yoludur.

Wi-Fi işlemleri , şu yetki değişikliğini içerir ; Dinamik erişim hakları atayan NAC ürünleri. En çok tutulan portal işlemleri. BYOD için ilk katılım ve cihaz kaydı. Güvenlikle ilgili manuel veya otomatik erişim hakları değişiklikleri.

Yetki değişikliğinin nedenleri arasında şunlar olabilir ; İlk bağlantıdan sonra kullanıcı veya uç nokta VLAN atamasında , ACL'de veya diğer erişim haklarında değişiklik. Güvenlik duruşunu kontrol eden NAC ürünü ile kullanıldığında uç noktanın duruşundaki değişiklik. NAC'de yazıcı için güvenlik kamerasına karşı farklı yetkilendirme sağlayabilen profil oluşturma işlemleri gibi uç noktanın kimliğinde değişiklik. MAC adresinde veya tanımlama için kullanılan diğer herhangi bir özellikte değişiklik , tipik olarak NAC senaryosunda. Kullanıcı veya uç nokta yaşam döngüsü yönetimi veya güvenlik izlemenin bir parçası olarak kullanıcının veya uç noktanın manuel olarak veya güvenlik entegrasyonları aracılığıyla otomatikleştirilmesinde değişiklik. İlk uç nokta kaydı veya BYOD yerleştirme yoluyla yetki değişikliği.

Yetki Değişikliği (CoA , IETF RFC 5176 , 8559'da tanımlanmıştır) , RADIUS sunucusunun ağ altyapısından bir uç noktanın bağlantısını kesmesini veya yetkilendirmesini değiştirmesini istemesine olanak tanıyan RADIUS uzantısıdır. CoA işlevi ; uç noktanın tanımlandığı ve üretim ağında kaydedildiği , muhtemelen karantinaya alındığı için birkaç yetki değişikliğine uğrayabileceği NAC dağıtımlarında yaygın olarak kullanılır. Kullanıcının oturum açıp açmadığına ve kullanıcının hangi erişim haklarına sahip olduğuna bağlı olarak değişikliklere uğrayabilir. NAC ürünlerinin bir uç noktanın yetkilendirme düzeyindeki değişiklikler hakkında kararlar alması için güvenlik duruşu ve profil oluşturma kullanılabilir. CoA işlevleri genellikle cihaz kaydı için olanlar (genelde NAC ürünü aracılığıyla) veya bir kullanıcının sertifikaların dahil edilmesi sırasında portal ile etkileşime girdiği BYOD iş akışı gibi çeşitli yerleştirme iş akışlarında kullanılır. Daha sonra güvenli ağa yönlendirilir. Çeşitli satıcıya özel tescilli özelliklerle genişletilmesine rağmen CoA'nın temel işlemi , RADIUS sunucusunun altyapı cihazına (doğrulama sunucusuna ACK (onaylandı)) veya NACK (olumsuz alındı) mesajı iletmektir.

COA RADIUS KODU	COA PAKETİ	AÇIKLAMA
40	Disconnect-Request	VLAN değişiklikleri için kullanılan uç noktanın bağlantısını kesmek için RADIUS sunucusundan altyapı cihazına gönderilen istek.
41	Disconnect-ACK	Altyapı cihazından RADIUS sunucusuna gönderilen başarılı bağlantı kesme onayı.
42	Disconnect-NAK	Altyapı cihazından RADIUS sunucusuna gönderilen negatif (başarısız) bağlantı kesme onayı.
43	CoA-Request	Uç noktaya yetki değişikliği yapmak için RADIUS sunucusundan altyapı cihazına gönderilen istek.
44	CoA-ACK	Altyapı cihazından RADIUS sunucusuna gönderilen yetkilendirmenin başarılı bir şekilde değiştirildiğinin alındısı.
45	CoA-NAK	Altyapı cihazından RADIUS sunucusuna gönderilen yetki değişikliğinin olumsuz (başarısız) onayı.

Uç nokta için tam bağlantı kesme ve CoA arasındaki fark ; Uç nokta VLAN'ının değiştiği durumlarda belirginleşir ve uç noktayı yeni DHCP isteği yapmaya zorlamak için tam bağlantı kesme / yeniden bağlanma gerekebilir. Aksi takdirde , uç nokta , onu her şeyden etkin bir şekilde izole eden IP adresi ve ağ geçidi bulunan VLAN'da bırakılabilir. Diğer RFC'ler altında , bağlantının kesilmesinin veya CoA'nın neden başarılı olmadığıyla ilgili iletişimler için başka uzantılar vardır. Bu değiş tokuşlar , hangi oturumun değiştirildiğini belirlemek için RADIUS özniteliklerini kullanır. Bağlantıyı kesme veya CoA isteği bir oturumla eşleşmezse , istek başarısız olur. Birden fazla oturumla eşleşirse , tüm oturumlar bağlantı kesme veya CoA işleminden etkilenir. CoA protokolünde mimari amaçlar için bilmeye değer olan şey , tüm ürünlerin tüm CoA işlevlerini eşit olarak desteklemediğidir. Bazı ürünler , temel CoA paketini Satıcıya Özel Nitelikler ile genişletirken , diğer ürünler CoA işlemleri için destek sağlamaz veya çok sınırlı destek sunar. Cisco'da bazı ürünler , önceden tanımlanmış RADIUS sunucusunda CoA'yı etkinleştirme seçeneğine sahipken , Juniper Mist gibi diğerleri ayrı olarak yapılandırılmış CoA / DM sunucu parametrelerine sahiptir.

Satıcı CoA Desteği ; Satıcıya Özel Nitelikler ile işlemleri daha da genişletir. Meraki ve benzeri ürün sınıfları gibi küçük-orta ölçekli işletme kullanım örneklerinden gelişen ürünler , kablolu veya kablosuz ağlarda CoA ile sınırlamalara sahip idi. Satıcıların neredeyse her zaman bu ve diğer standartlar için özellikler ve destek eklediğini söylemek doğru olur. Bu nedenle bir ürün seçmeden önce CoA desteği hakkında bilgi almanız yeterlidir. CoA beklendiği gibi çalışmıyorsa , satıcı desteğinize danışın.

Kimlik Doğrulama için EAP Yöntemleri ; Genişletilebilir Kimlik Doğrulama Protokolü (EAP) , kullanıcı adı-parola kimlik bilgileri veya cihaz sertifikaları gibi çeşitli kimlik doğrulama yöntemlerine uyabileceğimiz bir çerçevedir.

RADIUS ve EAP protokolleri birden çok amaç ve ağ sınıfı (taşıyıcılar ve hücresel dahil) için kullanıldığından , çeşitli IETF RFC'lerinde tanımlanmış sayısız EAP yöntemi vardır ve bu liste kullanım durumları ile birlikte büyümeye ve değişmeye devam edecektir. Amaçlarımız doğrultusunda , ağ ve kablosuz kimlik doğrulamasında kullanılan en yaygın EAP yöntemlerine odaklanmalıyız.

EAP-PEAP ve EAP-TLS , günümüzün ağ ve Wi-Fi kimlik doğrulamalarında iki ana standart tabanlı EAP yöntemidir. Çoğu zaman , " PEAP , kullanıcı adı ve parola kullanan Microsoft özelliğidir " ve " TLS , cihaz sertifikalarını kullanır " kabul edilir. Bu tamamen yanlış olmasa da tamamen doğru da değildir. En iyi güvenlik için çoğunlukla birleştirilen birçok dış ve iç mekanizma kombinasyonu vardır. Dahili kimlik doğrulama yöntemlerinin çoğu (EAP-TLS bir yana) gizlilik için tasarlanmamıştır yani kullanıcı adı ve kimlik bilgilerinin bir kısmını veya tamamını açık metin olarak iletebilirler. Bu kimlik doğrulamaları daha sonra güvenli bir tünelden geçirilerek en iyi şekilde korunur (VPN'lere benzer). Hepsi yaygın olarak kullanılmasa da , hemen hemen her iç ve dış kombinasyonu IETF RFC'leri tarafından desteklenir. EAP-PEAP tüneli içinde EAP-TLS göndermek tamamen mümkündür.

Dış EAP Tünelleri ; Kimlik doğrulama alışverişlerinin kendileri her zaman varsayılan olarak şifrelenmediğinden , uç nokta ve kimlik doğrulama sunucusu arasındaki kimlik bilgisi alışverişlerinin gizliliğini ve bütünlüğünü sağlamak için EAP iç kimlik doğrulamaları TLS ile güvenli tünellerin içine sarılır. Bu TLS tüneli , kimlik doğrulama sunucusunun sertifikası kullanılarak oluşturulur. Güvenli tünellerin amacı (tüm uygulamalarda) , kullanıcı adı veya kimlik dahil olmak üzere kullanıcı kimlik bilgilerinin uç noktadan iletilirken bütünlüğünü ve gizliliğini sağlamaktır. Bu korumayı sunmayan önceki EAP uygulamaları kullanımdan kaldırılmıştır ve kullanılmamalıdır.

EAP-PEAP ; PEAP (Korumalı EAP) başlangıçta RSA , Microsoft ve Cisco üyeleri tarafından ortak bir projeydi ve 802.1X kimlik doğrulaması için en yaygın olarak desteklenen tünelli (teknik olarak kapsüllenmiş) tür olarak kabul edilir. Tüm büyük işletim sistemlerinde yerleşiktir ve MSCHAPv2 ve EAP-TLS'nin yanı sıra Microsoft'a ait olmayan EAP yöntemleri de dahil olmak üzere çeşitli dahili kimlik doğrulama yöntemleriyle kullanılabilir. Microsoft PEAP , hem uç nokta hem de kimlik doğrulama sunucusunda etkinleştirildiğinde, kimlik bilgilerini önbelleğe alarak 802.1X ile güvenli bir ağda daha hızlı dolaşımı kolaylaştıran hızlı bir yeniden bağlanma seçeneği sunar.

EAP-TTLS ; EAP-TTLS (Tünelli Aktarım Katmanı Güvenliği) , EAP-TLS'nin dış şifreli tünel ekleyen bir uzantısıdır fakat EAP-TLS'nin aksine uç noktalar için cihaz sertifikaları gerektirmezler. Güvenli TLS tüneli kurulur ve ardından EAP-TLS , EAP-MSCHAPv2 gibi iç kimlik doğrulama yöntemi kullanılabilir. Uç nokta aygıt sertifikasıyla kimlik doğrulaması yapıyorsa (iç yöntemi olarak EAP-TLS aracılığıyla) , güvenli tünel aracılığıyla kullanıcı adı tabanlı kimlik bilgilerini ve sorgulamaları değiştirmek için ek aşamalar olmadan karşılıklı kimlik doğrulama tek bir aşamada gerçekleşebilir. EAP-TTLS , hızlı yeniden bağlanmayı da destekler. EAP-TTLS ve EAP-PEAP arasındaki fark son derece incedir ve PEAP'nin tam EAP değiş tokuşlarının kapsüllenmesi olarak tanımlanan nüansı ile ilgilidir.

Oysa EAP-TTLS , farklı RADIUS özniteliklerinin (özellikle EAP-TTLS , AVP veya Nitelik-Değer Çiftleri olarak referans verildiğini görebileceğiniz genişletilmiş RADIUS niteliklerinin kullanımını tanımlar. Güvenlik açısından birisi yeni bir saldırı oluşturana kadar) bunları eşdeğer kabul edin ve standartlara dayalı tünelli bir EAP yöntemi arıyorsanız , ortamınızda en iyi desteklenen kullanınız.

EAP-FAST ; EAP-FAST (Güvenli Tünel üzerinden Esnek Kimlik Doğrulama) , daha yaygın olan EAP-PEAP'ye benzer fakat dolaşımı kolaylaştırmak için farklı mekanizmaya sahip Cisco'nun tescilli bir uygulamasıydı. EAP-FAST , Korumalı Erişim Kimlik Bilgisi (PAC) biçiminde tanımlama bilgisi stili belirteci kullanır. EAP-FAST tüneli artık IETF RFC 4851'de tanımlanan bir standarttır. PAC belirteci , başarılı cihaz kimlik doğrulamasının kanıtı olarak kabul edilir ve 802.1X ile güvenli ağda dolaşım sırasında yeniden kimlik doğrulama gecikmesini önler. EAP-FAST , hem kullanıcıyı hem de cihazı doğrulamak için kimlik bilgileri zincirini de destekler. TTLS ve PEAP gibi EAP-FAST , EAP-MSCHAPv2 , EAP-GTC ve EAP-TLS gibi çeşitli dahili kimlik doğrulama yöntemleriyle kullanılabilir.

EAP-TEAP ; EAP-TEAP (Tünelli EAP) , cihaz ve kullanıcı kimlik doğrulamasını kolaylaştırmak için EAP kimlik bilgileri zincirini destekleyen Cisco'nun EAP-FAST'ına benzer başka standartlara dayalı EAP tünelidir. EAP-TEAP , neredeyse tüm diğer yaygın EAP tünel yöntemlerinde bulunmayan ortadaki adam saldırılarına karşı çeşitli güvenlik geliştirmeleri ve azaltmaları içerir. 2014'ten beri onaylanmıştır. Şu anda yalnızca maliyetli NAC ürünlerinde veya gelişmiş AAA sunucularında bulunan zincirleme kimlik doğrulama düzeyini sağlamak için yerel , standartlara dayalı bir fırsat sunacaktır. Yavaş yavaş benimseniyor ancak kablosuz güvenlik mimarisine harika bir katkı olacaktır. Cisco ISE ve Aruba ClearPass Policy Manager gibi kurumsal AAA ve NAC ürünlerinin şu anda EAP-TEAP ve kimlik bilgisi zincirini desteklediğini belirtmekte fayda var ancak bu ürün sınıfı , EAP-TEAP gerektirmeden aynı etkiyi elde etmek için ilkelerde zincirleme mantıksal ifadeler kullanabilir. EAP dış tünel yöntemlerinin karşılaştırması EAP-FAST ve EAP-TEAP , ek araçlar veya ürünler gerektirmeden yerel kimlik bilgileri zincirinin (hem kullanıcının hem de cihazın kimliğini doğrulamak için) ek avantajını sunar.

EAP TÜNEL	ENDÜSTRİ ADAPTASYONU	ZİNCİRLEME DESTEĞİ	GÜVENLİK
EAP-PEAP	Yaygın benimsenme.	Hayır.	Şifreli TLS kapsülleme.
EAP-TTLS	Yaygın benimsenme.	Hayır.	Şifreli TLS kapsülleme.
EAP-FAST	Az benimsenme. (Cisco Tescilli)	Evet.	MSK ile şifreli + Kriptografik bağlama.
EAP-TEAP	Düşük benimsenme.	Evet.	EMSK ile şifreli + Kriptografik bağlama (en iyi koruma).

EAP Desteğini Özelleştirme ; Microsoft ve diğer birçok popüler işletim sisteminde , EAP-PEAP veya EAP-TTLS dışında herhangi bir yöntem kullanıyorsanız , yükleyici veya üçüncü taraf sağlayıcı aracılığıyla uç noktaya diğer yöntemler için destek eklemeniz gerekir. Son noktaya ek EAP yöntemleri için destek eklemiş olsanız bile , bu ayarları Grup İlkesi veya MDM araçları aracılığıyla aktaramayabilirsiniz. Windows ortamındaki bazı standart olmayan EAP yöntemleri için EAP yöntemi etki alanının Grup İlkesi'nde desteklenmiyorsa , etki alanına katılmış uç noktalarda EAP yöntemleri bir seçenek olarak kullanılamaz. XML içeriğini dışa aktarma , değiştirme ve yeniden içe aktarma yoluyla Microsoft Grup İlkesi için geçici çözümler vardır. Microsoft PowerShell DSC (İstenen Durum Yapılandırması) kullanımı başka bir seçenektir. Son olarak , tüm RADIUS sunucuları yerel olarak tüm EAP yöntemlerini desteklemezler. Planlama ve tasarımınızda bir EAP yöntemine geçmeden önce 802.1X bağlantılı öğeler genelinde desteği doğrulayınız.

Tünelli EAP'nin Güvenliğini Sağlama ; Burada basitleştirilmiş olmasına rağmen tünelli EAP'ler için birçok katman ve saldırılara karşı değişen dayanıklılık seviyeleri vardır. Birçok tünelli EAP işlemi , dış tünel ve iç kimlik doğrulama yöntemi arasında kriptografik bağlama sunmaz. Bu da kötü niyetli bir kullanıcının bunları bir uç nokta ve altyapı cihazı olarak ortasına enjekte ettiği ortadaki adam saldırılarını mümkün kılar. IETF içinde uzun süredir devam eden çalışmalar , özellikle verilerin kablosuz olarak iletildiği ve bu nedenle gizli dinleme yoluyla saldırılara daha açık olan Wi-Fi ağları için EAP kimlik doğrulama yöntemlerinde kalan güvenlik açıklarının çoğunu çözmek için devam etmektedir. EAP-TEAP , iç ve dış kimlik doğrulama taraflarının aynı olmasını ve birinin saldırgan olmamasını sağlamak için daha sıkı EMSK tabanlı kriptografik bağlama gibi ortadaki adam saldırıları için halihazırda birkaç azaltıcı etkiye sahiptir. EAP-FAST , kriptografik bağlama sunmasına rağmen , saldırganın Kimlik Doğrulayıcı olarak görev yapan altyapı cihazını (RADIUS NAS cihazı) yanıltma yaptığı ortadaki adam saldırılarına karşı etkisiz olduğu kanıtlanmış MSK tabanlı kriptografik bağlama ile yapar. Bir iç yönteme dış yöntem olarak da izin verildiğinde ek güvenlik açıkları ortaya çıkar. Sunucuyu yapılandırırken izin verilen EAP yöntemlerine ilişkin önerilere özellikle dikkat etmenin nedenlerinden biridir. Birçok BT uzmanı , MSCHAPv2'yi iç kimlik doğrulama yöntemi olarak tünelsiz kimlik doğrulama yöntemi (güvenli değil) olarak tanımlar. İkincisi ise ortamı bir dizi saldırıya açar. Buradaki rehberlik , mükemmelliğin ilerlemenin düşmanı olmasına izin vermemektir. 802.1X güvenliği olmayan ağlardan güvenli EAP yöntemlerinden herhangi birine geçiş , güvenlikte büyük bir artış olacaktır. Çeşitli EAP tünel yöntemlerinde bulunan güvenlik açıklarının küçük ayrıntıları ve iç ile dış yöntemlerin ilişkileri , yanlış yapılandırmalar veya kötü tasarım nedeniyle ortaya çıkan güvenlik açıklarının yanında sönük kalıyor. Kötü niyetli aktörler tarafından hedef alınması muhtemel bir kuruluş veya endüstri türünde değilseniz , burada çevre için erişilebilir olan EAP yöntemiyle başlayınız.

Yüsek Güvenlikli Ortamlarda EAP ; Belirli küresel finans kurumları ve devlet kurumları gibi hedef alınması muhtemel kuruluş için çözüm tasarlıyorsanız , ek araştırma ve test yapılması gerekir. EAP ve TLS protokollerindeki güvenlik açıklarının araştırılması zamanla gelişir ve bu nedenle , son derece hassas uygulamalar için mimari yapan profesyoneller , o sırada mevcut verilere dayalı olarak riski değerlendirmelidir. IETF RFC'leri ve bilgi notları , kimlik doğrulama protokollerinin işleyişi hakkında zengin bilgilerin yanı sıra bunların eksikliklerinin ve güvenlik açıklarının ayrıntılı analizini sağlar. Bu alandaki güvenlik araştırmacılarından gelen en güncel verilerle birleştiğinde , mimariler ve protokoller hakkındaki kararları bilgilendirecektir. Uygulanan tüm çözümler penetrasyon testi yapılmalıdır (ideal olarak bu tür testlerde uzmanlaşmış , kullanıma hazır araçlar kullanmayan üçüncü tarafça) ve bilinen güvenlik açıkları belgelenmelidir. Başka yollarla azaltılmalı veya yoksa izlenmeli ve uyarılmalıdır. Alternatif olarak , birçok durumda , Wi-Fi bağlantısı için VPN'lerin kullanılması gibi daha yüksek bir güvenlik düzeyi için diğer teknolojiler birleştirilir.

İç Kimlik Doğrulama Yöntemleri ; İç kimlik doğrulama yöntemleri , dış tünel yöntemlerinden birinin içine sarılabilir veya bazı durumlarda kendi başlarına kullanılabilir. Tünel , kimlik bilgilerinin kimlik doğrulama işlemi sırasında açığa çıkmasını önler. Dahili yöntemler , kimlik bilgisi veya sertifika tabanlı olabilen , uç noktanın sunucuya nasıl kimlik doğrulaması yaptığını açıklar. Kimlik doğrulama sunucusu , her zaman bir sunucu sertifikasıyla uç noktaya kimlik doğrulaması yapar. Bu yaygın iç yöntemler daha önce RFC özelliklerine göre açıklanan dış tünellerin her biri tarafından desteklenir fakat tüm satıcıların her kombinasyonu desteklediği anlamına gelmez. Kimlik doğrulama sunucuları ve uç nokta işletim sistemleri üreticileri , yeni EAP desteği eklemek için yazılım sürümlerini düzenli olarak güncelliyor. Mevcut iç EAP yöntemlerinin çoğunun dış tünel ile kullanılması şiddetle tavsiye edilir ve açık (şifrelenmemiş) kimlik bilgilerine sahip olanlar yalnızca güvenli tünel içinde kullanılmalıdır.

İÇ DOĞRULAMA	DOĞRULAMA TİPİ	Tünelsiz Şifreleme	Önerilen Dış Tünel
EAP-TLS	Sertifika.	Evet.	EAP-TTLS
EAP-MSCHAPv2	Kullanıcı şifresi.	Hayır. Açık metin.	EAP-PEAP ve EAP-TTLS
EAP-GTC	Token	Hayır.	EAP-PEAP ve EAP-TTLS
EAP-POTP	Token	Evet.	Gerekli değil.

Standart dahili kimlik doğrulama yöntemlerinin dışında , kendi başına geçerli olan gerçekten yalnızca bir tanesi vardır ve o zaman bile tünellenmesi önerilir. Bu protokol EAP-TLS'dir.

EAP-TLS ; EAP-TLS (Aktarım Katmanı Güvenliği) karşılıklı sertifika kimlik doğrulamasını temel alarak şifrelemeyi içerir. Bu da dış tüneli isteğe bağlı kılar ancak yine de önerilir. EAP-TLS , burada bahsedilen dış yöntemlerden herhangi birinde tünellenebilir. Protokol TLS 1.0 gibi zayıf şifreleri desteklediğinden ve sürümü seçmek uç noktaya bağlı olduğundan , EAP-TLS ile dış tünel önerilir. Sürümü sunucu tarafından zorlamanın bir yolu yoktur. Güvenli dış tünelin hafifletilmesini eklemek veya uç noktaları güvenli TLS sürümlerini kullanacak şekilde yapılandırmak isteyeceğiniz anlamına gelir. EAP-TLS , cihaz sertifikaları ve dolayısıyla PKI altyapısı gerektirir. PKI altyapısı , etki alanı içinde Microsoft AD Sertifika Hizmetlerini etkinleştirmek ve hem sunucular hem de etki alanı uç noktaları için otomatik kaydı ayarlamak kadar basit olabilir veya PKI altyapısı , altyapıya ek yapılandırma ve entegrasyon gerektirebilecek üçüncü taraf çözüm olabilir.

Microsoft İstemcilerinde TLS Versiyonlarının Zorlanması ; TLS sürümü istemci tarafından seçildiğinden yalnızca en son sürümlere izin vermek için seçenekleri araştırmak isteyebilirsiniz. Microsoft ortamıyla çalışıyorsanız , TlsVersion adlı DWORD değerini tanımlayarak uç noktaları belirli TLS sürümlerini kullanacak şekilde yapılandırabilirsiniz. TLS sürüm 1.2 için tanımlanacak değer “0xC00” dur.

EAP-MSCHAPv2 ; EAP-MSCHAPv2 (Microsoft Challenge El Sıkışma Kimlik Doğrulama Protokolü sürüm 2) , kullanıcı adı-parola kimlik bilgileriyle kimlik doğrulaması yapar ve daha önce açıklanan tünel korumalı dahili bir yöntem olarak veya kendi başına belirtilebilen EAP yöntemlerinden biridir. Ancak tünelli bir koruma ile her zaman kullanılmalıdır. EAP-MSCHAPv2'nin kimlik doğrulama sırasında kimlik bilgilerinin kullanıcı adı kısmını şifrelemediğini hatırlayınız. Microsoft uygulamalarında MSCHAPv2 , bir süre sonu ilkesi gerektirdiğinde kullanıcının parolasını güncellemesine olanak tanır. Bir karışıklık noktası , MSCHAPv2'nin RADIUS sunucusu ve uç nokta yapılandırmalarında nereye uyduğunu anlamaktır.

EAP-GTC ; EAP-GTC , belirteçler ve tek seferlik parola (OTP) platformlarının yanı sıra LDAP dahil olmak üzere çeşitli kimlik depoları için genel kimlik doğrulamalarını destekleyen iç yöntemdir. Esnek olmasına rağmen GTC yaygın olarak desteklenmez veya kullanılmazlar. Yine de gerekirse GTC , sadece açık metin veya Microsoft NT hash’leri değil , aynı zamanda tuzlu (salt) ve tuzsuz (unsalted) MD5 ve SHA1 hash’leri olan parolalara sahip veritabanlarını destekleyebilir.

EAP-POTP ; Benzer işlevler için RSA tarafından geliştirilen ve donanım tabanlı USB bağlantılı belirteçlere uygun özelliklere sahip EAP Korumalı Tek Kullanımlık Parola (POTP) gibi özel EAP yöntemleri de vardır. EAP-POTP gibi daha yeni özel protokoller , saldırılara karşı ek koruma için kanal bağlama ve karşılıklı kimlik doğrulama gibi ek güvenlik yararları (EAP-GTC üzerinden) ve parola girmek için insan müdahalesinin ortadan kaldırılmasını sağlayabilir.

Eski ve Güvenli Olmayan EAP Yöntemleri ; Çeşitli IETF RFC'lerinde tanımlanmış , bazıları taşıyıcı kullanımı için bazıları hücresel kullanım için ve diğerleri LAN ile Wi-Fi kimlik doğrulaması için kullanılan fakat artık kullanımdan kaldırılan veya sadece tünelli bir yöntem içinde kullanılması gereken çok sayıda EAP yöntemi vardır.

Bunlar şunları içerir ; EAP-MD5 (tamamen kullanımdan kaldırıldı) , EAP-LEAP (tamamen kullanımdan kaldırıldı) , EAP-PAP (şifrelenmemiş , dış tünel olmadan kullanmayın , LDAP için gerekli) , EAP-CHAP (şifreli ancak savunmasız , dış tünel olmadan kullanmayın) , EAP-MSCHAP (şifreli ancak savunmasız , dış tünel olmadan kullanmayın).

Genel olarak , bu kullanımdan kaldırılmış ve güvenli olmayan EAP yöntemlerinden kaçınınız. Hepsinin bilinen güvenlik açıkları vardır ve burada sunulan diğer yöntemlerin yaygın desteğiyle , bunların hiçbirini altyapınızda desteklemeye gerek yoktur. Kullanımdan kaldırılan protokolleri (MD5 ve LEAP) hiçbir koşulda asla kullanmayınız. Diğerleri için daha eski kimlik doğrulama yöntemini kullanmak için iş gereksiniminin olduğu bir durum varsa , bunun bir tünelde ve son derece hassas ortamlarda korunduğundan emin olunuz. Bu cihazlara güvenli değillermiş gibi davranmanızı ve segmentlere ayırmanızı önerilir.

EAP-PAP ve CHAP kimlik doğrulama sınıfları , altyapının diğer bölümleri (SSL-VPN veya cihaz yöneticisi kimlik doğrulaması gibi) için kullanılabilir ve bu nedenle RADIUS ilkelerinde mevcut olabilir fakat kablosuz ağda kimlik doğrulaması yapan kullanıcılar için kullanılmayacaktır. . 802.1X güvenli ağlar istediğiniz kadar EAP yöntemini barındırabilse de , güvenli ve güvenli olmayan protokolleri aynı SSID üzerinde birleştirmeyiniz. Çünkü bu , ortamı grup anahtarlarından yararlananlar da dahil olmak üzere bir dizi içeriden saldırıya açar.

Güvenli Wi-Fi için Önerilen EAP Yöntemleri ; EAP yöntemleri en yaygın olarak kullanılan , desteklenen ve önerilen temel kümeye indirgenmiş olsa da , sindirilecek ve organize edilecek çok şey vardır. Uygulaması en kolay / en hızlı olandan başlayıp biraz daha ilgili entegrasyonlara doğru ilerleyen önerilerin kısa bir özetini yapacak olursak ; Yazma sırasında , uzun süredir fakat EAP-TEAP ortam genelinde destekleniyorsa , kimlik bilgileriyle , sertifikalarla veya her ikisiyle kimlik doğrulamak isteyip istemediğinize bakılmaksızın bu en güvenli ve esnek seçenektir. Kullanıcı adı-parola kombinasyonlarını kullanmayı tercih ediyorsanız ve Microsoft ortamındaysanız , MSCHAPv2 iç ve hızlı yeniden bağlantı etkinleştirilmiş EAP-PEAP dış , en kolay ve en güvenli seçeneğinizdir. Cihaz sertifikalarını kullanabilecek durumdaysanız , EAP-TLS iç ile EAP-TTLS dışı idealdir. Yalnızca EAP-TLS kullanıyorsanız , istemci tarafında güvenli TLS sürümlerini zorlamanız faydalı olacaktır. Cihaz sertifikaları birçok kişi tarafından en güvenli uygulama olarak kabul edilir fakat kötü niyetli bir kullanıcı sertifikaya sahip cihaza sahipse hala güvenlik açıkları vardır ve bu nedenle mümkün olduğunda ikili veya zincirleme kimlik doğrulamayı tercih edebilirsiniz. Cihazın değil , sadece kullanıcının kimliğinin doğrulanmasıyla ilişkili güvenlik açıkları da vardır. Bu nedenle zincirleme kimlik doğrulamaları veya mantıksal ifadeler ekleyebilen RADIUS sunucusu şiddetle tercih edilir. Hem kullanıcıyı hem de cihazı doğrulamanız veya doğrulamanız gerekiyorsa , PKI altyapınız yoksa veya cihaz sertifikaları vermemeyi tercih ediyorsanız , politikada zincirleme veya iç içe mantıksal ifadeleri destekleyen NAC ürünü veya gelişmiş AAA sunucusu kullanınız. AND işlevi şu anda Microsoft NPS'de desteklenmemektedir. Hem kullanıcının hem de cihazın kimliğini doğrulamanız gerekiyorsa ve PKI altyapınız varsa , ortamınızda destekleniyorsa tekrar EAP-TEAP'ı seçmelisiniz veya alternatif olarak EAP-FAST , cihaz sertifikası tabanlı kimlik doğrulama için EAP-TLS ile kullanıcı kimlik bilgileri tabanlı kimlik doğrulama için EAP-PEAP / MSCHAPv2 kombinasyonunu kullanınız. Belirteçleri içeren özel kullanım durumlarınız varsa , EAP-POTP veya EAP-GTC'yi tek başına veya EAP-TEAP , EAP-FAST veya NAC ürünü veya gelişmiş AAA sunucusu kullanarak zincirleme veya mantıksal yapılandırmada kullanınız. Daha önce ele alınmayan ve dikkate alınabilecek diğer bir EAP yöntemi ise IETF RFC 5421'de tanımlanan EAP-FAST-GTC'dir.

DIŞ TÜNEL	İÇ EAP	KULLANIM ALANLARI	NOTLAR
EAP-TEAP	Herhangi	Yaygın değil.	İç / dış güçlü kriptografik bağlama , kimlik bilgileri zincirini destekler.
EAP-PEAP	MSCHAPv2	Windows AD için çok uygun.	Tüm Platformlarda desteklenir. Kimlik doğrulama gerekmez.
EAP-TTLS	EAP-TTLS	Sertifika tabanlı PKI.	Geniş destek ve kullanıcı doğrulama gerekmez.
yok	EAP-TLS	Sertifika tabanlı PKI.	Dış tünel olmadan şifrelenir fakat TTLS önerilir.

EAP-TEAP- EAP-FAST ; EAP-TLS / MSCHAPv2 , NAC olmadan kim. bilgisi zincirleme. , EAP-TEAP standarttır. Kriptografik bağlamalar yoluyla en güvenlidir. Yaygın olarak desteklenmez.

Herhangi Herhangi NAC varsa TEAP/FAST olmadan doğrulama. NAC ürünleri çeşitli özelliklere sahiptir fakat kullanıcıyı / cihazı doğrulamaya izin veren özellik vardır.

EAP-PEAP/ EAP-TTLS ; EAP-GTC , Gösterişsiz belirteç uygulaması , Geniş destek , doğal güvenlik yoktur. Mümkünse POTP kullanın.

Yok " none " ; EAP-POTP , Daha güvenli jeton uygulaması. , Daha sağlam özellikler, manuel kullanıcı müdahalesi gerekmez ve dış tünel olmadan şifreleme içerir.

MAC Tabanlı Kimlik Doğrulamaları ; MAC adresi kullanımının kullanıcı veya cihaz kimlik doğrulaması değil , tanımlama biçimi olduğunu unutmayınız. Infosec dünyasında , kimlik doğrulamanın kimliği doğrulayarak (kanıtlayarak) genişletirken , kimliğin bir kimlik iddia etme süreci olduğu yaygın olarak kabul edilir. Kablosuz mimaride MAC kimlik doğrulamasının görünmesinin birkaç yaygın yolu vardır ; RADIUS ile MAC Kimlik Doğrulama Baypas (MAB) , 802.1X olmayan uç noktaların RADIUS kullanarak 802.1X ile güvenli ağda kimlik doğrulaması yapması için geçiş mekanizmasına izin verir. RADIUS'suz MAC Kimlik Doğrulaması , RADIUS tabanlı olmayan kimlik doğrulama ve zorlamayı destekleyen ürünlerle ağ erişim denetimi (NAC) dağıtımlarında tipiktir. MAC filtreleme , reddetme listesi ve izin verilenler listesi , ağ altyapısından belirli uç nokta MAC adreslerini filtreleme (izin verme , vermeme) yeteneğinden bahseder.

RADIUS ile MAC Kimlik Doğrulama Atlaması ; Kablolu veya Wi-Fi dağıtımları için MAC Authentication Bypass (MAB) ile 802.1X kullanımını vardır. Bu yöntem , 802.1X'e katılmayan uç noktaların Enterprise / 802.1X ile güvenli ağa bağlanmasına , kimlik doğrulaması yapmasına izin verir. Mükemmel dünyada , tüm uç noktalar 802.1X ile kimlik doğrulaması yapabilecektir. Neredeyse mükemmel bir dünyada sadece 802.1X ile kesinlikle kimlik doğrulaması yapamayan cihazlar MAB gibi bir yöntemi kullanır. Ve gerçek dünyada MAB , yazıcılar ve VoIP telefonları gibi 802.1X'i destekleyebilen geleneksel olmayan uç noktalarda karmaşık yapılandırmalardan kaçınmak için kolaylık olarak kullanılır. Herhangi bir satıcıyla , 802.1X bir bağlantı noktasında yapılandırıldığında , MAB'ye izin verilmesini ve yeniden kimlik doğrulama zamanlayıcıları , kimlik doğrulama zaman aşımları , izin verilen durumlar (sadece MAC adresi izin verilen veya birden çok ve nasıl birden çok işlenir). Bu durumda bir bağlantı noktası bir anahtardaki fiziksel bir uç bağlantı noktası veya bir Wi-Fi sistemindeki mantıksal SSID bağlantı noktası anlamına gelebilir. Yıllar içinde , MAB'nin , özellikle Cisco ISE veya diğer RADIUS tabanlı NAC ürünleri kullanımdayken , 802.1X ağlarının işlevinin bir parçası olduğu varsayıldığı Cisco ortamlarında son derece yaygındır. Tersine , güvenlik bilincine sahip kuruluşlarda MAB'yi bir mimarinin parçası olarak desteklenir fakat nadiren tasarlamaya dahil edilir.

MAB'I Seçen Satıcılar ; Cisco ve birkaç seçkin diğer satıcının neden MAB'yi tercih ettiğini merak ediyor olabilirsiniz. 802.1X/ EAP dağıtımları RADIUS kimlik doğrulama sunucularına dayanarak birçok satıcı (Cisco ve Aruba Networks dahil) NAC ürünlerinde (sırasıyla ISE ve ClearPass Policy Manager olarak) sağlam kimlik doğrulama hizmetleri sunar. Son derece sağlam olmakla birlikte , bu iki ürün özellikle RADIUS tabanlı olmayan kimlik doğrulama ve zorlama için tasarlanmamıştır. Teknik olarak Aruba CPPM , bu amaç için tasarlanmış OnConnect adlı bir özelliğe sahiptir fakat müşteriler onu kullanmaktan uzaklaştırılır ve henüz geniş ölçekte çalışmazlar. Cisco ISE ve öncülleri de RADIUS tabanlı olmayan kimlik doğrulama sunmazlar. 802.1X olmayan cihazlar için bile RADIUS kimlik doğrulamasına dayanır ve bu nedenle kurumsal ortamlarda 802.1X olmayan uç noktaların sayısız istisnasını ele almak için MAB'ye ihtiyaç duyar. RADIUS tabanlı kimlik doğrulama ve zorlamaya dayanan ürünler , RADIUS dışında ağ altyapısıyla etkileşim kurmak için bir mekanizmaya sahip değildir. Alternatif olarak , RADIUS tabanlı olmayan uygulamaları destekleyen ve mükemmel olan ürünler vardır. Bunlar arasında ForeScout ve Fortinet FortiNAC bulunur. RADIUS'a ek olarak SNMP , CLI veya API'ler aracılığıyla altyapıyla etkileşim kurmak için RADIUS tabanlı olmayan zorlama desteği seçenekleri sunan ürünlerdir. Wi-Fi ağlarında daha az önemlidir fakat kablolu bağlantı noktalarında bağlantı noktası erişim kontrolü için kritik bir farklılaştırıcıdır.

Tipik MAB İşlemlerine Genel Bakış ; Yüksek düzeyde MAB , altyapı cihazının (AP veya denetleyici gibi) uç nokta adına (MAC adresini kullanarak) kimlik doğrulama isteği oluşturmasını sağlayarak çalışarak kimlik doğrulama için RADIUS sunucusuna gönderir. Çalışması için ağ cihazının , bağlantı noktasında veya SSID bağlamında uygulanan bir şey olan MAB işlemlerine izin verecek şekilde yapılandırılması gerekir. MAB'nin operasyonlarının detayları bundan sonra biraz bulanıklaşıyor çünkü MAB , 802.1X'in aksine standart değildir. Her satıcının kendi MAB uygulaması vardır. MAB için farklı RADIUS öznitelikleri kullanır ve MAB çevresinde farklı yardımcı ayarlar sunar. Satıcıların MAB uygulamalarında birkaç ortak tema ve güvenlik düşüncesi vardır. Etkinleştirildiğinde , uç noktanın MAC adresi , MAC adresine eşit kullanıcı adı ve parolanın kimlik doğrulaması için kullanılır. Dizinde RADIUS'un kimlik doğrulaması yapması gereken bir kullanıcı hesabı olmalıdır. İşlem sırası şöyledir ; Uç nokta , 802.1X güvenli ağa bağlanır ve ağ ile EAPoL'u başlatması istenir. Uç nokta , EAPoL isteğine yanıt vermiyor ve genelde üç denemeden sonra yanıt alınamıyorsa ağ cihazı , yapılandırılmışsa MAB'ye geçecektir. Ağ cihazı , kullanıcı adı ve parola olarak uç noktanın MAC adresini kullanır ve RADIUS sunucusuna bir kimlik doğrulama isteği oluşturur. RADIUS sunucusu , ilkede belirtilen dizine göre kimlik bilgilerini arar (örneğin Active Directory veya NAC ürünü). MAC tabanlı kullanıcı hesabı eşleşirse , başarılı bir kimlik doğrulama döndürülür ve uç noktaya izin verilir. Arıza durumunda çıkmaz veya yalnızca internet VLAN'ı belirtilebilir.

MAC İşlemlerinin Satıcı Varyasyonları ; MAB herhangi bir standartta tanımlanmadığından , satıcılar bunu genel parametreler dahilinde uygun gördükleri yöntemle uygularlar.

Satıcılar arasında MAB'deki bazı yaygın varyasyonlar şunları içerebilir ; Farklı RADIUS öznitelik alanlarının kullanımı (arama istasyonu kimliği , parola , oturum açma gibi). Farklı kimlik doğrulama protokollerinin kullanılması (PAP , CHAP , EAP-MD5 veya tescilli). Karar verme için NAC özelliklerinin eklenmesi (cihaz profili oluşturma veya güvenlik duruşu analizi gibi). Ağ cihazı ve kimlik doğrulama sunucusu arasındaki iletişim sarmalayıcı (homojen ortamlarda özel uygulamaları içerebilir). Kimlik doğrulama zaman aşımları , yeniden kimlik doğrulama ayarları ve mod için yapılandırma seçenekleri (tekli veya çoklu MAC adresleri). Muhtemelen etki alanı altyapısı , harici veritabanı veya NAC ürünleri içindeki veritabanı içinde , uç nokta veritabanının değişen havuzları.

MAB için Güvenlik Hususları ; MAB kötü bir seçenek değildir fakat genelde kurumsal ağın güvenlik beklentileriyle orantılı bir şekilde uygulanmazlar. Kesinlikle , MAB'yi herhangi bir güvenlik mimarisine gereksiz ek olarak düşünmeyin fakat MAB'yi dahil etmeyi planlıyorsanız , mimaride dikkate alınması gereken bazı hususlar şunlardır ; MAB , RADSEC veya satıcıya özel bir uygulama ile kullanılmadıkça güvenli olmayan korumasız kimlik doğrulama protokolleri (CHAP ve MD5) kullanır. MAB , aynı kullanıcı adı ve parolaya izin veren bir kullanıcı parolası ilkesi gerektirir MAB , infosec ve uyumluluk tanımlarına göre kimlik doğrulama değildir. Saldırganlar , EAPoL yanıtlarını saklayarak ve sahte MAC adresi kullanarak kolayca MAB geçersiz kılmayı zorlayabilir. MAB , dinamik VLAN'ları iyi işlemeyebilir. MAB , MAC sahtekarlığına karşı koruma sağlamaz. MAB için satıcı güvenlik özellikleri ek ürünler veya lisans gerektirebilir. Yazıcılar ve ağa bağlı diğer cihazlar dahil olmak üzere birçok uç nokta 802.1X'i destekler. MAB, 802.1X ile aynı şifreleme ve anahtar yönetiminden faydalanmaz.

802.1X ve MAB'de güvenliği etkileyen bazı farklılıkları vurgulamaktadır. 802.1X güvenli varlıkları MAB ile bağlanan uç noktalardan ayırmak gereklidir. Aynı kablosuz ağdalarsa , ayrı VLAN'larda olsalar bile kablosuz olarak bir yayın alanını paylaştıklarını unutmayınız.

802.1X vs. MAB güvenlik farkları ;

Kimlik Doğrulama ; Güçlü karşılıklı kimlik doğrulama. (802.1X) Sadece MAC adresiyle uç nokta tanımlaması. (MAB)

Şifreleme ; Güçlü şifreleme ve anahtar döndürme. (802.1X) Parola korumalı ağa eşdeğerdir. (MAB)

Bütünlük ; Düzgün şekilde uygulanırsa kimlik bilgileri , kimlik doğrulama sırasında güvence altına alınır. (802.1X) Kimlik bilgisi, kablosuz olarak Wi-Fi paketlerinde açık metin olarak geçirilen MAC adresidir. (MAB)

Standart ; 802.1X ve EAP için IEEE ve IETF standartları tarafından tanımlanmıştır. (802.1X) Standart, satıcıya bağlı uygulama ve değişkenlik yoktur. (MAB)

Güvenlik ; Düzgün uygulanırsa yüksek. (802.1X) Düşük. (MAB)

MAB İçin Güvenlik Ve Şifreleme ; MAB , 802.1X güvenli bağlantı noktasındaki bir alt yapılandırma olduğundan , MAB bağlantılarının 802.1X bağlantılarıyla aynı şekilde şifrelendiğini varsayılır fakat durum böyle değildir. MAB uç nokta iletişimleri , Kişisel veya parola korumalı bir ağın eşdeğeri ile kablosuz olarak güvence altına alınır. 802.11'in çalışma şeklinden dolayı , uç noktaların MAC adresleri havadan açık metin olarak iletilir ve basit dinleme ile kolayca keşfedilir. Uç noktanın yakınında bulunan kullanıcı veya uygulamanın MAC adresini kolayca yakalayabileceği , uç noktanın MAC adresini taklit edebileceği ve ağa erişim kazanabileceği anlamına gelir. Profil oluşturma kurallarını erişim ilkelerine dahil edebilen NAC ürünlerinde ve kimlik doğrulama sunucularında bunun için bazı hafifletmeler vardır fakat çoğu ortamda bu katmanlı denetimler standart değildir.

MAB Kullanırken Öneriler ; MAB , Wi-Fi ağına belirli düzeyde güvenlik kontrolleri uygulamak için gerçekten son bir çaba olmalıdır. MAB , mimarinizin zorunlu bir parçasıysa , bu öneriler mümkün olan en yüksek güvenliği sunacak ve 802.1X korumalı varlıklarınızı koruyacaktır.

MAB Yetkili Cihazları için Üretim Ağlarından Ek Segmentasyon Ekleyiniz ; MAB bağlantılı cihazlar , 802.1X kimlik doğrulamalı uç noktalarla SSID veya VLAN paylaşmamalıdır. MAB , hiçbir şekilde kimlik doğrulama , profil oluşturma veya duruş değerlendirmesi sunmazlar. MAC adresi kimliğiyle bağlanan uç noktalar , tamamen 802.1X güvenli uç noktaları olan üretim ağlarına gelmemelidir. Uç noktanın 802.1X ağı üzerinden bağlanmasına izin verilmiş olması , güvenlik gereksinimlerini karşıladığı anlamına gelmez. RADIUS , dinamik VLAN'lar ve ACL'ler gibi dinamik öznitelikler döndürebilirken , MAB cihazlarının IP adresini düzgün şekilde serbest bırakmayabileceğini ve yenilemeyebileceğini unutmayın.

MAB'nin Kendi RADIUS İlkesini Kullanmasını Sağlayınız ; MAB daha az güvenli kimlik doğrulama protokolleri kullandığından , MAB cihazları için farklı bir ilke yapılandırarak 802.1X kimlik doğrulamalı uç noktalarınızın bütünlüğünü koruyun ve sadece bu ilke üzerinde daha az güvenli protokollere izin veriniz. İlkenin sadece MAB cihazlarına izin verdiğinden ve 802.1X ile kimlik doğrulaması yapabilen , yapması gereken normal kullanıcı veya bilgisayar hesaplarına izin vermediğinden emin olunuz.

MAB Uç Noktaları için Ayrı Dizin Grubu Oluşturun; MAB aygıtlarını özel bir dizin grubuna yerleştirmek , RADIUS ilkesinde başvurabileceğiniz kapsayıcı ve gereken parola ilkesi değişiklikleri gibi diğer değişikliklerle ayrıntılı yol sağlar.MAB uç noktalarının kullanıcı hesapları olması gerekir ve çoğu uygulamada kullanıcı adı ile parola hem uç noktanın MAC adresidir.

Dizin Hizmetlerinde Parola Politikası Değişikliği ile Ayrıntılı Olunuz ; Kurumsal etki alanı politikaları , kullanıcılar için güçlü parolalar talep ederek çoğu , özellikle kullanıcı adıyla eşleşen parolalara izin vermezler. Etki alanına MAB kullanıcı hesapları ekliyorsanız , o grup için parola güvenlik gereksinimlerini azaltan çok ayrıntılı bir politika oluşturmanız gerekir.

Güvenlik Açıkları için Satıcının Uygulamasını Test Ediniz ; Her satıcının MAB tadı farklı olacaktır ve satıcılar ürün yazılımı güncellemelerinde davranış değişiklikleri getirebilir. MAB , operasyonun kuruluşun güvenlik beklentilerini karşıladığından emin olmak için ağın yaşam döngüsü boyunca test edilmeli ve yeniden test edilmelidir. Şirket içi testlere ek olarak , üçüncü taraf kalem testi de şiddetle tavsiye edilir ve bu testlerin sonuçları , yapılandırmak için ek izleme ve uyarı konusunda bilgilendirmeye yardımcı olabilir.

MAB'yi izleyiniz ; Tüm ağlar fakat özellikle MAB gibi bilinen güvenlik açıkları olan ağlar izlenmelidir. SIEM veya kullanıcı ve varlık davranışı analitiği (UEBA) ürünleriyle ilgili anormallikleri izleyiniz.

Profil Oluşturma ve MAC Sahtekarlığını Önleme için bir NAC Ürünü kullanınız ; Daha yüksek düzeyde güvenlik ve MAC sahtekarlığını önlemek için dinamik uç nokta profil oluşturma kurallarını katmanlamak için NAC çözümü kullanınız. Profil oluşturma kuralları , açık bağlantı noktaları DHCP parmak izlerini , HTTP başlıklarını , SNMP'yi veya diğer parametreleri beklenen değerle karşılaştırarak uç nokta profillerini inceler.

Her Şeyi Yükselt ; Eski RADIUS sunucuları , MAB cihazları için şifrelerin geri dönüşümlü şifreleme kullanılarak saklanmasını gerektiriyordu ve bazı ağ cihazları , kullanımdan kaldırılmış EAP-MD5 kullanıyor. MAB kullanmanız gerekiyorsa , daha iyi güvenlik için altyapı bileşenlerini mümkün olduğunca güncelleyin ve yükseltiniz.

802.1X için Uç Nokta Desteğini Kontrol Ediniz ; Yazıcılar ve VoIP telefonları gibi yaygın uç noktalar yıllardır 802.1X'i destekliyor. MAB'den memnun olmadan önce uç nokta envanterini kontrol ederek MAB'den 802.1X'i destekleyen uç noktaları geçiriniz. Bazıları yazılım veya bellenim yükseltmeleri gerektirebilir fakat bu cihazların büyük bir yüzdesinin MAB'ye ihtiyaç duymama olasılığı yüksektir. 802.1X ve MAB , bağlantı noktası düzeyinde bağlamda yapılandırılır. Wi-Fi'de bu tam bir SSID'dir ancak bir anahtarda bunlar ayrı uç bağlantı noktası komutlarıdır. 802.1X'i kablolu ağ üzerinde yönetmek , kablosuz bir sistemden çok daha karmaşıktır. Kuruluşlar 802.1X'i kablolu bağlantı noktalarına uygulamaya çalıştığında çoğu NAC uygulaması başarısız olur ; bu durum ya uygun beklentiler ve planlama ile ya da RADIUS tabanlı olmayan uygulama çözümleri kullanılarak önlenir.

RADIUS Olmadan MAC Kimlik Doğrulaması ; MAB , 802.1X ve RADIUS'a güvenirken , RADIUS gerektirmeyen MAC kimlik doğrulama çözümleri de vardır. RADIUS tabanlı olmayan kimlik doğrulama ve zorlamayı destekleyen ürünler , kimlik doğrulama ve yetkilendirme hakkında kararlar almak için altyapı cihazlarını ve ilke motorunu (çoğunlukla NAC sunucusu) kullanır. Düzgün yapılandırıldığında , NAC tabanlı çözümler , MAB dağıtımlarına göre çeşitli güvenlik avantajları sağlar ; Kurumsal 802.1X dağıtımlarından ödün vermezler. MAC adreslerine sahip dizin kullanıcı hesapları gerektirmezler ; uç nokta dizini NAC sunucusunda depolanır. Dizin ilkelerinde daha az güvenli parola ilkeleri oluşturulmasını gerektirmezler. Daha az güvenli kimlik doğrulama protokollerinin etkinleştirilmesini gerektirmezler. İkili 802.1X açık / kapalı davranışı değil , ayrıntılı uygulama sunarlar. MAB uç noktaları için bile VLAN değişikliklerini sorunsuz şekilde desteklerler. MAC sahtekarlığı olasılığını büyük ölçüde azaltan gelişmiş uç nokta profili oluşturma ve mekanizmalar sunarlar. Çoğu ürün , katılım ve cihaz kaydı sunar. Bağlantı noktası düzeyinde yapılandırma gerekmediğinden kablolu zorlama için kolayca kullanılabilirler.

MAC Filtreleme ve Reddetme ; MAC adreslerini reddetme listeleri aracılığıyla filtrelemek , kurumsal Wi-Fi ürünlerinin ortak özelliğidir. Başka kimlik doğrulama değil protokolü , MAC reddetme listesi için güvenlik uygulamaları olduğundan burada bahsetmeye değerdir. Çoğu zaman bunlar ; SIEM , IPS veya diğer algılama , yanıt motoru gibi güvenlik ürünüyle entegrasyon yoluyla dinamik olarak uygulanır. MAC reddetme listeleri ile kablosuz altyapı , kablosuz sistem içindeki filtrelemeyi zorlar. MAC filtrelemenin kullanım durumu , parola korumalı ağa bağlanabilen uç noktaları sınırlamak için denetimler eklemektir. Elde taşınır tarayıcılar ve kimlik doğrulamayı desteklemeyen diğer geleneksel olmayan uç noktalar gibi cihazları destekleyen ağlar için yaygındır. Statik MAC filtreleme , NAC gibi daha iyi kontroller veya MAB gibi diğer MAC tabanlı yetkilendirmeler tercih edilerek uygulamalardan yavaş yavaş kaybolmaktadır. MAC filtreleme (MAB ve belirli NAC yetkilendirmeleri ile birlikte) dahil olmak üzere MAC tabanlı kontrolleri kaçınılmaz olarak engelleyecek olan MAC rastgeleleştirme çağının başlangıcındayız.

Kimlik Doğrulama ve Tutsak Portallar için Sertifikalar ; Ağ kimlik doğrulaması ile ne zaman , nerede , nasıl ve hangi tür sertifikaların kullanılacağı , çarpık ve genellikle yanlış anlaşılan konu gibidir.

Kablosuz altyapıyla ilgili sertifikalar ve kimlik doğrulama için yaklaşık beş kullanım durumu vardır ; son kullanıcıların kimliğinin doğrulanması , uç nokta cihazlarının kimliğinin doğrulanması , yönetici kullanıcıların kimliğinin doğrulanması , sunucuların kimliğinin doğrulanması ve kablosuz altyapı bileşenlerinin kimliğinin doğrulanması. bir başkasına.

802.1X için RADIUS Sunucu Sertifikaları ; 802.1X standardı , karşılıklı kimlik doğrulamayı tanımlar ; hem kimlik doğrulama sunucusunun hem de uç noktanın birbirine kimlik doğrulaması yapması gerektiği anlamına gelir. Uç noktalar sertifika kullanmıyorsa sunucunun da sertifika gerektirmediğine dair yaygın yanılgı vardır. AAA işlevlerini gerçekleştiren RADIUS sunucusu , her zaman , kesinlikle, zamanın yüzde 100'ünde , kendisini uç noktalarda doğrulamak için sunucu sertifikası gerektirir. Uç noktalar , kullanıcı kimlik bilgileri (kullanıcı adı ve parola) aracılığıyla MSCHAPv2 (iç) ile EAP-PEAP (dış) aracılığıyla kimlik doğrulaması yapsa bil e, sunucu yine de ve her zaman sertifika kullanarak uç noktada kimliğini doğrular.

Çeşitli EAP yöntemleri için sunucu sertifikası gereksinimleri; ;

İÇ EAP DOĞRULAMA	Endpoint Doğrulama	Sunucu Doğrulama
EAP-TLS	Sertifika	Sertifika
EAP-MSCHAPv2	Kullanıcı adı ve şifre	Sertifika
EAP-GTC / EAP-POTP	Token	Sertifika
herhangi	herhangi	Sertifika

Kullanılan sunucu sertifikası özel sertifika olmalıdır (joker karakterli sertifika olmamalı) ve çoğu durumda , dahili etki alanı tarafından verilen sertifika olmalıdır.

Sertifika Talepindeki Adımlar ; X.509 tabanlı sertifikalar asimetrik (genel / özel) anahtarları kullanır ve birçok biçimde olabilir. Sertifika oluşturma işlemi birkaç bileşen ve dosya içerecektir. Sertifika imzalama isteği (CSR) oluşturmak ve sertifikaları yüklemek için kimlik doğrulama sunucunuzdan (RADIUS veya sabit portal) gelen talimatları izleyiniz. Bu süreç boyunca özel anahtar dosyasıyla birlikte sertifika alacaksınız. İndirdiğiniz özel anahtar dosyası , her yerde tek kopyadır. Tıpkı bir parola gibi güvenli yerde saklayınız ; kimlik bilgisi kasası veya güvenli depolama alanı idealdir ; Sertifikaya ihtiyaç duyan sunucudan veya sunucu için CSR oluşturunuz. Sertifikalar , tam nitelikli alan adıyla (FQDN) verilir , IP adresleri artık desteklenmiyor. Sertifika yetkilisinden (CA) sertifika istemek için CSR'yi kullanınız. CA , genel ve özel anahtarla birlikte bir sertifika dosyası yayınlayacaktır. Sertifika dosyasını ve özel anahtarı kullanarak sertifikayı sunucuya yükleyiniz. Özel anahtarı güvenli bir yerde saklayınız. Kaybederseniz ve daha sonra ihtiyacınız olursa , tüm bu işlemi tekrarlamanız gerekir.

802.1X kimlik doğrulaması için sunucu sertifikaları ; Sunucu sertifikasına , kimlik doğrulaması yapan uç noktalar tarafından güvenilmesi gerektiğidir. Uç noktaların şirket tarafından yönetildiği ve dolayısıyla etki alanının üyeleri olduğu standart Windows ortamında , bu önemsiz bir görevdir çünkü RADIUS sunucusu genelde Microsoft NPS'dir ve Microsoft sertifika yetkilisine otomatik olarak kaydedilir. Bu sertifika , etki alanına katılan tüm uç noktalar tarafından otomatik olarak bilinecek ve güvenilecektir. Öte yandan , henüz etki alanına katılmamış uç noktalara sahip dahili olarak verilen etki alanı sertifikası kullanıyorsanız , ek adımlar gerekir ve bu dahili sertifikanın uç nokta yapılandırma sistemi aracılığıyla uç noktaya iletilmesi gerekir. MDM aracı gibi veya kullanıcı tarafından manuel olarak yüklenir. Bu senaryo , kendi cihazını getir (BYOD) kullanım durumlarında veya uç noktaların halihazırda etki alanı üyesi olmadığı herhangi bir senaryoda en yaygın olanıdır ; birleşme ve satın almalar sırasında kimlik doğrulamasını diğer etki alanlarına genişleterek , etki alanı olmayan işletim sistemi platformlarını destekler. Ortamın tamamı Windows değilse , buradaki iki gereksinim vardır ; kimlik doğrulama sunucusunun geçerli sunucu sertifikasına sahip olması ve bu sertifikanın , o ağda kimlik doğrulaması yapan uç noktalar tarafından bilinmesi ve güvenilmesi gerekir.

KSS VE SAN Sertifikalarını Kullanma ; Windows ortamına sahip küçük ve orta ölçekli kuruluşlarda , Windows Server'daki otomatik kayıt özellikleri sayesinde dahili etki alanı sertifika yetkilisi , sunucu sertifikaları , cihaz sertifikaları ile birkaç dakika ila birkaç saat içinde çalışmaya başlamak mümkündür. Daha büyük ortamlarda ve üçüncü taraf RADIUS sunucusu veya NAC ürünü kullanan ortamlarda , ister 802.1X ister sabit portal ihtiyaçlarını destekleyin , ek adımlar olacaktır. Daha büyük ve dağıtılmış dağıtımlar , birden çok RADIUS sunucusu veya sabit portal sunucusu için destek gerektirebilir. Kullanılan üründen ve işleme veyahut yük dengeleme algoritmasından bağımsız olarak , tüm olası kimlik doğrulama sunucularında ağı kapsayacak şekilde tek sertifika kullanmak ortak bir istektir. Özellikle pahalı , genel olarak imzalanmış sertifikalar kullanan sabit portalları dağıttığımızda yararlıdır. Joker karakter sertifikalarını asla kullanmayınız. Birden çok sunucuyu kapsayan sertifika istiyorsanız , Konu Alternatif Adı (SAN) sertifikalarını kullanarak bir grup sunucu için sertifika verme seçeneği vardır. SAN sertifikası almak için sertifika imzalama isteğinin (CSR) istenen alternatif adları belirtmesi gerekir. Bazı ürünler , CSR sürecinde SAN sertifikalarının talep edilmesini yerel olarak desteklerken , diğerleri desteklemez. Ürününüz bunu desteklemiyorsa , bu amaca hizmet edecek hazır birçok ücretsiz Linux aracı vardır. 802.1X'te olduğu gibi dahili alan kullanımı için genelde aynı maliyet avantajı yoktur fakat seçenek olarak olması harikadır.

802.1X için Uç Nokta Cihaz Sertifikaları ; Sunucunun her zaman bir sertifikası olması gerekirken , uç nokta cihazları sertifika veya belirteç , kullanıcı adı-şifre kimlik bilgileri gibi alternatif yollarla ağda kimlik doğrulaması yapabilir. EAP-TLS veya benzeri sertifika tabanlı kimlik doğrulama kullanılıyorsa , uç noktanın elbette sertifikaya ihtiyacı olacaktır. Sunucu sertifikalarında olduğu gibi kesinlikle gerekli olan yalnızca iki öğe , uç noktanın geçerli bir sertifikaya sahip olması ve kimlik doğrulama sunucusunun bu sertifikayı doğrulamak için havuza erişiminin olmasıdır. İptal parametreleri gibi sertifika güvenliği için daha sonra ele alınacak başka seçenekler ve en iyi uygulamalar vardır. Cihaz sertifikalarının kullanımı , Ortak Anahtar Altyapısı (PKI) gerektirir. Temel Microsoft ortamında , hem sunucular hem de uç noktalar için kaydı otomatikleştirmenin birçok yolu vardır. Bu da sertifika verme ve yükleme sürecini oldukça kolaylaştırır. Genelde organizasyonun , doğrudan homojen Microsoft dağıtımının mümkün olmadığı veya istenmediği büyüklükte veya sektörde olduğu durumlar vardır. Kuruluş , Windows olmayan işletim sistemlerini destekleyebilir. BYOD veya yüklenici destek gereksinimleri olabilir ve merkezi olarak yönetilmeyen uç noktalar veya IoT , endüstriyel IoT (IıoT) ve operasyonel teknoloji (OT) gibi standart olmayan işletim sistemleri olabilir.

IoT ; Sağlık hizmetleri ortamları , mükemmel IoT test yerleridir. Hastaneler , ana teknoloji haline gelmeden önce IoT kullanıyordu ve Gıda ve İlaç Dairesi (FDA , Amerika Birleşik Devletleri) tarafından belirli bir konfigürasyonla onaylanabilen biyomedikal cihazlarla karmaşık uç nokta ekosistemleri için harika bir örnek teşkil ediyorlardı. Bazen eski işletim sistemlerine bağlı ve genelde sistemi yönetmek veya izlemek için sözleşmeli üçüncü taraflarca desteklenir ve kilitlenir. Bu durumlarda , yalnızca mümkün olmakla kalmaz , aynı zamanda bazı biyomedikal cihazlara , amaca yönelik olarak oluşturulmuş CA tarafından sertifika verilmesi de son derece olasıdır. Genelde otonom sistemler , düzenleme ve iptal de dahil olmak üzere cihaz sertifikasının tüm yaşam döngüsünü yönetir. Karşılıklı sertifika tabanlı kimlik doğrulama (EAP-TLS ile olduğu gibi) kriptografik olarak en güvenli olanı olsa da , ona bağlı kullanıcıyı doğrulamadan uç noktanın kimliğini doğrulamaktan kaynaklanan güvenlik açıkları olduğunu unutmayınız. MSCHAPv2 gibi parola tabanlı kimlik doğrulama yöntemlerini çevreleyen güvenlik açıkları , dış tünelin ayrılmasını ve iç kimlik doğrulamasını hedefleyen belirli saldırılarla ilgili olup, bazı belirli ortadaki adam saldırılarını mümkün kılar. EAP yöntemleri , iç ile dış arasındaki kriptografik bağlama için güncellendiğinden , bu güvenlik açıkları kaybolacak ve yenileri ortaya çıkacaktır. Sertifikalar her zaman daha iyidir şeklindeki düşünce tarzı , kriptografik bütünlüğe rağmen mutlaka doğru değildir. Hem uç noktanın hem de kullanıcının kimliğinin doğrulanması doğru olandır fakat bu mümkün olmadığında , kuruluş ; kullanıcıyı mı yoksa cihazı mı doğrulamanın daha önemli olduğu konusunda riske dayalı bir karar vermelidir. Her birinin artıları ve eksileri var.

802.1X için Sertifikaları Kullanmak İçin En İyi Uygulamalar ; Sertifika verme ve yönetme konusunda öğrenilecek çok şey vardır. 802.1X dağıtımlarının tümü olmasa da çoğu için geçerli olan bazı kolay en iyi uygulamalar vardır.

Joker Karakter Sertifikalarını Asla Kullanmayın ; Joker karakter sertifikaları tam olarak göründükleri gibidir. FQDN'nin bir bölümünde kullanılan bir * (yıldız) ve etki alanının alt etki alanının o sertifika ile geçerli olacağını gösterir. Bu nedenle , *.xxx.com joker sertifikası, " test1.xxx.com" ve " test2.xxx.com " ile " test3-xxx.com " , " test4.xxx.com " ve temel olarak xxx.com hakkında düşünebileceğiniz her şeydir. Korkunç güvenlik açığı olmanın yanı sıra , joker karakter sertifikaları çoğu RADIUS sunucusu için genelde kabul edilmezlar. Sunucu , sertifikayı yüklemenize ve bunu RADIUS ilkesinde belirtmenize izin verir fakat günlüklerde herhangi bir neden belirtilmeden kimlik doğrulama başarısız olur. Diğerlerinin yanı sıra Microsoft NPS , joker karakter sunucu sertifikalarının kullanımına izin vermeyen bir sunucudur. Oldukça sinir bozucu ve güvenli değildir , bu nedenle her zaman joker karakter sertifikalarından kaçınınız. Bunun yerine , amaç birkaç bileşen için tek bir sertifikaya sahip olmaksa SAN sertifikaları kullanınız.

Kendinden İmzalı Sertifikaları Asla Kullanmayınız ; Kendinden imzalı sertifikalar , sunucu (bu bağlamda genelde üçüncü taraf yazılımı) kendisine sertifika verdiğinde ortaya çıkar. Bunu yaparken sertifika , dahili veya genel olmayan güvenilir kök CA'dan verilmezler. Birçok işletim sistemi , bir kullanıcının kendinden imzalı sertifikalardan gelen güvenlik uyarılarını atlama seçeneğini sistematik olarak kaldırmaya başlamıştır. Kendinden imzalı sertifika seçenekleri genelde üçüncü taraf yazılımlarda ve altyapı cihazlarında görünür. Joker karakter sertifikası kötüyse , kendinden imzalı sertifika kullanmak daha da kötüdür. Bir laboratuvarda bile dahili kök CA hizmetlerini başlatmak veya genel imzalı sertifikaları kullanmak daha iyi olur. Kendinden imzalı sertifikalar büyük olasılıkla çalışmayacaktır ve çalışsalar bile kendinizi veya kuruluşunuzu ek güvenlik açıklarına karşı savunmasız duruma getiriyorsunuz demektir. Dahili etki alanı altyapınızı ve özellikle RADIUS veya AD hizmetlerinizle aynı platformda Sertifika Hizmetlerini etkinleştirdiğiniz Windows Server ortamını göz önünde bulundurarak , RADIUS NPS'ye etki alanından sertifika yayınlayarak kök CA , kendinden imzalı sertifika olarak kabul edilmezler. Uç noktanın güvenebileceği ve doğrulayabileceği kök CA'ya sahip meşru bir sertifikadır.

LET'S ENCRYPT'ten ücretsiz sertifika alma ; Kendi dahili sertifikalarınızı oluşturma seçeneğiniz yoksa , kamu yararına çalışan ücretsiz , otomatik ve açık sertifika yetkilisi olan Let's Encrypt'e göz atmalısınız. İnternet Güvenliği Araştırma Grubu (ISRG) tarafından sağlanan bir hizmettir ve Cisco , Mozilla , EFF , Chrome , Meta , AWS , Akamai ve diğer düzinelerce teknoloji endüstrisi ağır topları tarafından desteklenmektedir.

Sunucu Sertifikalarını Daima Doğrulama ; 802.1X'in başlangıcından bu yana , çoğu uç noktada sunucu sertifikasını doğrulamama seçeneğini belirleme lüksüne sahibizdir. Bu seçim , sunucu sertifikasını tamamen yok sayarak sunucu sertifikasının geçerli mi yoksa güvenilir mi olduğunu doğrulamaz. Başlangıçta sorun giderme ve ilk 802.1X dağıtımlarıyla çalışan ağ yöneticileri için harika bir seçenek olan bu seçenek , kısa sürede ortadaki adam saldırılarına karşı güvenlik açığının kaynağı haline gelmiştir. 2019'dan bu yana , uç nokta platformları , kullanıcıların sunucu sertifikasını yok sayma seçeneğini yavaş yavaş kaldırmaktadır. WPA3 güvenliğinin daha geniş şekilde benimsendiğini ve 802.1X güvenli ağlarda sunucu sertifikalarını doğrulamak için ek gereksinimleri gördüğümüz için bu eğilim yalnızca 2022-2025 yılları arasında da devam edecektir. Test sırasında bile sunucu sertifikasını atlamak kötü bir fikirdir. Bunu kullanmanızı önerdiğim tek geçerli zaman , bazı aşırı sorun giderme veya acil durumlar içindir. RADIUS sunucusu , ilke oluşturma sırasında sizi sertifika seçmeye zorlayacağından , sunucuda geçerli sertifika olmalıdır. Var olabilecek boşluk , kişisel cihazlarda , BYOD'de veya etki alanında olmayan cihazlardan (bazı tabletler veya akıllı telefonlar gibi) gelen bağlantılarda sıklıkla meydana gelen uç noktanın bu sertifikayı bilmemesi veya güvenmemesi olabilir. Daha katı WPA3-Enterprise dağıtımlarında bile , halihazırda güvenilir değilse , kullanıcının sunucu sertifikasını manuel olarak kabul etmesine ve yüklemesine izin vermek için desteklenen mekanizmalar vardır. Test etme ve sorun giderme için fazlasıyla yeterli olmalıdır. Üretim ortamı hiçbir koşulda uç noktaların sunucu sertifikası doğrulamasını atlamasına izin vermemelidir. Normal işlemlerin ötesinde BYOD geçici çözümü ve test için bile izin vermemelidir.

Pentest Cihazları Sertifika Doğrulaması ; Wi-Fi'de görülen en büyük açıklardan en başlar da 802.1X ağları dağıtan ve sunucu sertifikasının doğrulamasını atlayan kuruluşlar vardır. Her durumda , kuruluşlar en iyi 802.1X güvenliğine sahip olduklarını düşündüler fakat bu gözden kaçan ayar , testçilerin ortadaki adam saldırısını kolayca başlatmasına ve güvenliği atlamasına olanak tanıyan bir güvenlik açığı ortaya çıkarmıştır.

RADIUS Sunucuları için Etki Alanı Tarafından Verilen Sertifikaları Kullanma ; RADIUS sunucuları için etki alanı tarafından verilen sertifikayı kullanmak için iki birinci sürücü vardır. Birincisi , genel olarak imzalanmış sertifikaların çoğunlukla bunlarla ilişkili maliyeti olması ve bu sertifikalar için maksimum geçerlilik süresinin giderek azalmasıdır. Yıllık yenilemeler için yüksek maliyetler anlamına gelir. Tek maliyet atlatması , okullar ve hükümetler gibi genellikle çok az veya hiç maliyet olmadan toplu satın alma pazarlığı yapan belirli kamu sektörü dağıtımlarındadır. İkinci sürücü güvenliktir ; kimlik doğrulama sunucularına etki alanı (dahili CA) tarafından verilen sertifikaları kullanmanın güvenlik avantajları vardır. Uç noktalara yalnızca bu sertifikalara veya bu ağ bağlantısı için etki alanı CA'sı tarafından verilen sertifikalara güvenmeleri istenebilir. Sunucu tarafından üçüncü taraf veya genel olarak imzalanmış sertifikaların kullanıldığı durumlarda , uç noktanın zaten bu genel CA için kurulmuş güven zincirine sahip olması mümkündür. Kullanıma hazır , uç noktalar bugün kullanılan en yaygın kök CA'lara güvenecek şekilde önceden yapılandırılmıştır ve bu nedenle doğal olarak genel CA tarafından verilen bir sertifikaya güvenirler. Dahili 802.1X / EAP kimlik doğrulaması için genel olarak imzalanmış sertifika kullanarak , ağı , saldırganın şirket ağının kötü ikizini başlatabileceği ve sertifikayı kullanabileceği başka bir ortadaki adam saldırısı senaryosuna açabilirsiniz. Kök CA zaten güvenilirdir. Uç noktalar , sadece bu saldırıyı azaltan ancak sertifikalar yenilendikçe veya yeniden yayınlandıkça yönetilemez hale gelebilecek belirli sertifikalara (genel olarak imzalanmış CA'dan) güvenmek üzere kilitlendiyse olur. Bu nedenlerle , dahili CA'nızdan RADIUS sunucu sertifikaları vermek ve bu ağa bağlanan uç noktaların yalnızca uygun CA'dan gelen sertifikalara güvenmesini sağlamak genelde daha kolay , daha güvenli ve çok daha uygun maliyetlidir. Teknolojideki her şey gibi , bu tavsiyeye bağlılık vardır ve bu emir vermelisin anlamına gelmez. Eduroam hizmetini kullanan , üçüncü bir taraftan sertifika veren ve sertifikaları tüm katılımcı kuruluşlarda geçerli olan okullar ve üniversiteler gibi dahili olarak verilen sertifikanın kullanılmasının mümkün olmadığı veya tercih edilmediği belirli kullanım durumları vardır. Uç noktanın Wi-Fi'ye bağlanmasına ve ardından etki alanına katılmasına izin vermek gibi genel olarak imzalanmış sertifika kullanmayı tercih eden standart kurumsal dağıtım senaryoları olabilir ; herhangi bir yerden planlanmamış çalışma sırasında yardımcı olur (WFA). Windows AD'de , bir bilgisayarı etki alanına bağlamak veya bilgisayarı ilk kez 802.1X ile güvenli ağa bağlamak için tipik süreç , BT personelini veya cihazı önce kablolu ağda sağlayan kullanıcıyı içerir. Sonraki güvenli Wi-Fi bağlantılarında kullanılan kimlik bilgilerinin önbelleğe alınmasına izin verir. Açıkçası , pandemi operasyonlarının dikte ettiği mevcut iklimde bu mümkün olmayabilir. Bununla birlikte , çoğu dağıtımda ve kesinlikle Microsoft'un eko-sisteminde , BT yönetici ekip üyesini ve kullanıcının geçici kablosuz profil yapılandırması için birlikte çalışmasını içeren , daha sonra kullanıcı tarafından üzerine yazılan tek seferlik önyükleme bağlantıları için daha güvenli geçici çözümler vardır.

Grup Politikasında Güvenilir Sertifikaların Yapılandırılması ; Başka sunucu eklerseniz veya orijinal sunucu sertifikasını güncellerseniz / yenilerseniz , uç nokta kimlik doğrulamasında başarısız olur. Bunun yerine , ilkeyi belirli kök sertifika veya kök CA yayınlayacak şekilde ayarlamayı seçebilirsiniz. Sertifika ayarları Grup İlkesi veya MDM tarafından kontrol edilir ve kilitlenirse , kullanıcı bu ayarları geçersiz kılamaz veya değiştiremez. Böyle bir durumda ise kullanıcılar siz politikayı değiştirene ve onları güncellenmiş politikayı alabilecekleri şekilde birbirine bağlayana kadar tepetaklak olacaktır. Yeni cihazlar için önyüklemeler olmasına rağmen uç noktanın zaten ayarlara erişimi kısıtlayan bir grup ilkesi varsa , önyükleme işlemlerini takip etmek mümkün olmayabilir. Kapak tarafında , ilkede hiçbir sunucu veya kök CA güveni tanımlanmadıysa , uç nokta , uç noktanın güvenilir kök CA deposundaki tüm kök CA'larla bağlantılara izin verir.

Özellikle Uç Nokta Sertifikaları için İptal Listelerini Kullanın ; PEAP ve MSCHAPv2 veya diğer belirteç ile parola tabanlı kimlik doğrulama , kimlik bilgileri günceldir veya değildir. RADIUS sunucusu , anında kabul veya reddetme sağlamak için çeşitli dizinlere bağlanır. Ancak , EAP-TLS gibi uç noktalardaki cihaz sertifikalarında , sertifika verildiği süre boyunca geçerlidir ve aksi iptal edilmediği sürece iyidir. Bu nedenle , doğrulama sunucularının bu bağlantıya izin vermeyeceğini bilmeleri için doğrulamayı zorlamak , sertifika doğrulama / iptalini kontrol etmek için bir yöntem kullanmak çok önemlidir.

Dahili olarak verilen sunucu sertifikasının sorun yaşaması ve iptal edilmesi olasılığı genelde daha düşük bir risktir fakat sertifikaları güvenli şekilde yönetmek , iptal de dahil olmak üzere tüm yaşam döngüsünün yönetilmesini gerektirir. Bir cihaz sertifikasına sahip uç noktanın , birkaç nedenden dolayı sertifikanın kaldırılması veya iptal edilmesi gerekebilir ; uç noktanın temel hazırlığı kaldırılmış olabilir , çalışan şirketten ayrılıyor olabilir , kullanıcının rolü ve erişim hakları değişiyor olabilir veya sertifikayı veren CA tarafından uç nokta sertifikasının güvenliğini geçersiz kılan ifşa olmuş olabilir. Uç nokta cihaz sertifikaları kullanıyorsanız , sertifika iptali için ürününüzün kılavuzunu izleyiniz. Tipik olarak , RADIUS sunucusu , büyük ve hacimli olabilen sertifika iptal listelerini (CRL) veya yalnızca CRL'lerdeki farklılıkları belirli aralıklarla aktarmak için diff işlemi kullanan delta CRL'leri kullanır. PKI mimarisi , bunun yerine , CRL denetimini boşaltan çevrimiçi sertifika durumu protokolünü (OCSP) kullanabilir. Süresi dolmuş sertifikaların iptal edilmediğini unutmayınız.

Sertifika Geçerlilik Sürelerinin Sözleşmesi ; Sertifikalarla uğraşmak yeterince karmaşık değilmiş gibi sertifika geçerliliğinde , sertifika planlama ve izleme sürecini daha da karıştırabilecek son değişiklikler olmuştur. İlk olarak , endüstri bizi FQDN'leri kullanmaya zorlayarak IP adresine dayalı konu adlarını desteklemeyi bırakmıştır. Ardından , SSL / TLS'de sektör genelinde yapılan değişiklikler , genel olarak verilen sertifikaların geçerlilik süresini en fazla iki yıla indirmiştir. Ancak daha yakın zamanlarda , bazı üreticiler tek taraflı olarak platformlarının yalnızca 398 gün veya daha kısa süreyle geçerli olan SSL / TLS sertifikalarına güveneceğine karar vermiştir. Bu yeni politika endüstri genelinde benimsenmedi ancak kesinlikle büyük bir kullanıcı ve cihaz popülasyonunu etkilemektedir. Bu kısıtlama , 1 Eylül 2020'de veya sonrasında oluşturulan sertifikalar için geçerlidir. Şu anda bu 398 günlük politika yalnızca tarayıcı tabanlı kısıtlamadır ve 802.1X tabanlı kimlik doğrulama için verilenler gibi etki alanı sertifikalarını etkilemez ancak etkileyecektir. Sabit portallar ve benzer kısıtlamalar , sertifika kullanımının diğer alanlarına sızabilir. Uygulamadan bağımsız olarak , sektör genelinde iki yıllık azami süre , kamuya açık herhangi bir sertifikaya uygulanır. 802.1X kimlik doğrulamasında kullanılan sertifikalar hakkında , hem RADIUS sunucusu (her zaman gereklidir) hem de cihaz sertifikaları (uç noktalar sertifikalarla kimlik doğrulaması yapıyorsa gereklidir) dahil olmak üzere , şimdiye kadar veya hiçbir zaman bilmek istemediğiniz her şeyi tamamlar.

Captive Portal Sunucu Sertifikaları ; 802.1X ile güvenli ağlar çoğunlukla yönetilen cihazlarda yönetilen kullanıcıların kimliğini doğrularken , sabit portallar çoğunlukla konuk kaydı için kullanılır. Misafirlere kabul edilebilir kullanım politikası , BYOD cihaz kaydı (yönetilmeyen uç noktalar için) ve diğer kişisel cihaz kayıtları için kullanılır. Sabit portallar doğrudan Wi-Fi altyapısında (kontrolörler veya AP'lerde) barındırılabilir veya harici sabit portal kullanabilir (Cisco ISE , Aruba ClearPass Policy Manager , Fortinet FortiNAC gibi NAC ürünlerine yeniden yönlendirme gibi) .

Captive Portallar için Sertifikaları Kullanmaya Yönelik En İyi Uygulamalar ; Captive portallar çoğunlukla Açık Sistem Kimlik Doğrulama ağlarıyla ilişkilendirilse de , Kişisel / parola güvenlikli veya Kurumsal / 802.1X güvenli ağ ile sabit portalı zorlamak tamamen mümkündür. Özel kullanım durumundan bağımsız olarak , sabit portal sertifikaları için kılavuz tutarlıdır.

Çoğu Durumda Genel Kök CA İmzalı Sunucu Sertifikası Kullanın ; Sabit portala bağlanan herhangi bir cihaz için kurumsal olarak yönetilen bir cihaz değilse (etki alanının bir üyesi veya kurumsal MDM tarafından yönetiliyorsa) , genel olarak imzalanmış sertifika kullanmak isteyeceksinizdir. 802.1X güvenli ağların çoğu için tam tersi bir öneridir. Bu konuk veya yönetilmeyen cihazlarda , dahili alan kök CA sertifikanız indirilmez ve güvenilmezler. Önceden kurulmuş ve güvenilen tüm ortak genel kök CA'lara sahip olacaklardır. Kenar çubuğu olarak MDM aracına uç nokta (akıllı telefon , tablet veya dizüstü bilgisayar) kaydederek ve sunucu sertifikasını göndererek çözülebilir.

MAC Randomizasyonunun Captive Portallar Üzerindeki Etkisini Anlama ; MAC önbelleğe alma , sadece başarılı portal tamamlamayı uç noktanın MAC adresine ekleyerek sonraki portal deneyimleri sırasında altyapı , uç noktayı işlemi zaten tamamlamış olarak tanımlar. MAC adresi herhangi bir noktada değişirse , altyapı bunun yeni bir uç nokta katılımı olduğunu düşünecek ve süreci yeniden başlatacaktır. MAC önbelleğe alma deneyimine sahip portal , uç noktanın ayarlarına bağlı olarak bozulabilir. MAC rastgeleleştirmesi yapılandırılabilir ve kullanıcı onu kullanmayı , kullanmamayı veya MAC adresinin ne sıklıkta değişeceğini seçebilir. Bundan daha derine inmek , bu seçenekler ve varsayılan ayarlar tüm platformlarda düzenli olarak değiştiği için verimli olmayacaktır.

Captive Portal Sertifikası En İyi Uygulamaları Özeti ; Sabit portallardaki sertifikalar için en iyi uygulamalar şöyledir ; Genel kök CA imzalı sunucu sertifikası kullanınız. Çoğu kullanım durumunda , uç noktanın başka yollarla önceden yüklemeden sunucu sertifikasına güvenmesi gerekeceğini biliniz. Tek kimlik doğrulama sunucusu veya kümesiyle bile birden çok sunucu sertifikasına ihtiyaç olabileceğini biliniz. Harici portal ve harici portala yeniden yönlendirilen Wi-Fi altyapısı üzerindeki sertifikalar kullanıldığında en iyi uygulama arasında olabilir. MAC adresi rastgeleleştirmesinin kullanıcı deneyimini ve arka uç işlemlerini etkileyebileceğini unutmayınız. Sabit portal işleminin DHCP , DNS , yönlendirmeler , erişim kuralları ve kritik zamanlayıcılar / zaman aşımı ayarları gibi bir dizi sahne arkası ağ işlemi içerdiğini unutmayınız. Sertifika Geçerlilik Sürelerinin daraltılması. Halihazırda kısıtlı geçerlilik süresi en fazla iki yıldır ve bazı uç noktalar , bir yıldan fazla geçerli sertifikalarla çalışmazlar. CSR'leri ve SAN sertifikalarını kullanmayınız. Bu , özellikle portal barındırma varlıkları , çoklu denetleyiciler , AP'ler veya diğer kimlik doğrulama sunucularından oluşan bir kümeye sahip daha büyük kuruluşlarda yararlıdır.

Kullanım durumuna göre sunucu sertifikası önerilerinin özeti ;

KULLANIM	SSID GÜVENLİK	ÖNERİ	NOTLAR
Yönetilen alan cihazındaki dahili alan kullanıcıları.	Enterprise/802.1X	CA tarafından verilen dahili bir sertifika kullanın.	Etki alanı bilgisayarları, dahili kök CA'ya zaten güvenecek
Yönetilmeyen alan cihazındaki dahili alan kullanıcıları ;	Enterprise/802.1X	CA tarafından verilen dahili bir sertifika kullanın ve sertifikayı bir MDM aracı aracılığıyla aktarın.	Alanın üyesi olmayan kişisel cihazlar, BYOD veya kurumsal cihazlar (ör. akıllı telefonlar) dahili sertifikanın yüklü olması gerekir.
Harici federe kullanıcılar (Eduroam gibi) ;	Enterprise/802.1X	Genel CA tarafından verilen bir sertifika kullanın.	Geçici ve federe kullanıcılar, etki alanı kök CA'sının doğal güvenine sahip olmayacaktır.
Misafir Portal ;	Açık veya Gelişmiş Açık.	Genel CA tarafından verilen bir sertifika kullanın.	Sorunsuz bir deneyim için portal, konuk kullanıcının cihazının zaten güveneceği bir sertifika kullanmalıdır.
Yönetilmeyen BYOD kayıt portalı ;	Açık veya Gelişmiş Açık.	Genel CA tarafından verilen bir sertifika kullanın.	En iyi katılım için portal, cihazın zaten güveneceği bir sertifika kullanmalıdır.

Captive Portal Güvenliği ; Birçok amaç için kullanılır ; Kullanıcı veya misafir kaydı. Kabul edilebilir kullanım politikalarının onaylanması. BYOD için uç nokta kaydı. Ücretli erişim için ödeme ağ geçitlerinin sunumu.

Her bir kullanım durumu , farklı güvenlik ve mimari ihtiyaçları beraberinde getirir. Kişisel / parola veya Kurumsal / 802.1X ağlarına bağlanan kullanıcıya sabit portal sunmak mümkün olsa da , bunlar çoğunlukla burada odak noktası olan Açık Sistem Kimlik Doğrulaması SSID'leri ile birlikte kullanılır.

Kullanıcı veya Misafir Kaydı için Captive Portallar ; En yaygın kullanım durumu olan sabit portallar , genelde konuk kullanıcıların sadece internete bağlı bir ağa erişmesine izin veren mekanizmadır. Konuk kaydı iş akışları , genelde kuruluşun güvenlik gereksinimlerine bağlı olarak birkaç yoldan biriyle yapılandırılır.

Doğrulama Olmadan Misafir Kendi Kendine Kaydı ; Bu türdeki captive portallar , konukların bilgilerin gerçek olduğuna dair herhangi bir doğrulama olmaksızın kendilerini kaydetmelerine olanak tanır. Birçok kuruluş için yeterlidir fakat bir olay durumunda denetim ve ilişkilendirme için ayrıntılardan yoksundur.

Doğrulamalı Misafir Kendi Kendine Kaydı ; Bu sabit portallar konukların kendilerini kaydetmelerine izin verir fakat en az bir tanımlanabilir bilgiyi doğrulamak için kimlik bilgilerini (şifre , bağlantı , oturum açma kodu) e-posta veya SMS metni yoluyla gönderir. Güvenlik bilincine sahip kuruluşlar için buradaki avantaj ; gerçek ve kullanıcı tarafından izlenebilir en az bir e-posta adresine veya telefon numarasına sahip olmalarıdır. İzlenmesi kolay olmasa da , insanların değişik isimlerde kaydolmalarını önlemek için genelde e-posta veya telefon numarası istemek yeterlidir.

Misafir Sponsorlu Kayıt ; Sabit portallardaki sponsorlu iş akışları , bir konuğun erişim talep etmesine izin verir ve daha sonra otomatik iş akışı (çoğunlukla e-posta tabanlı) aracılığıyla bir veya daha fazla izin verilen sponsor tarafından onaylanır. Kayıt seçeneklerinin en güvenlisidir. Misafir kullanıcı gerçek zamanlı olarak talepte bulunarak erişim gerektiğinde sponsor bunu gerçek zamanlı olarak onaylar. Günümüzün kurumsal Wi-Fi çözümlerinin çoğu , yerel olarak üründe veya NAC çözümleri gibi ek yazılımlar aracılığıyla sponsorlu iş akışları sunar.

Misafir Ön Onaylı Kayıt ; Kuruluş içindeki sponsorların konuk ziyaretçiyi önceden onaylamasına olanak tanıyan sabit portallar ile ön hazırlık yapma seçenekleri de vardır. Kimlik bilgileri , genelde e-posta veya SMS metin yoluyla ziyaretçiye önceden gönderilir. Sponsorlu kayıt iş akışına benzer şekilde , erişimin ön provizyonu genelde kullanıcı için e-posta adresiyle ve belirli bir tarih ve süre için belirtilir. İsteğe bağlı sponsorlukla karşılaştırıldığında , bu modelin iki dezavantajı vardır. Hesap , gerekenden daha uzun bir süre için tahsis edilebilir veya ziyaret iptal edilebilir , yeniden planlanabilir , bu da kimlik bilgilerinin ele geçirilmesi durumunda kötüye kullanım fırsatı doğurabilir. İkincisi gerçekten güvenlikle ilgili değil , provizyon sisteminde ziyaret sırasında yeniden provizyon gerektirebilecek zaman dilimi uyumsuzlukları veya diğer tuhaflıklar olması yaygındır. Açıkçası bu , ön onaylayan hesapların ek faydalarını ortadan kaldırır.

Misafir Toplu Kayıt ; Captive portallar , kuruluşun bire bir kimlik bilgilerinin verilmesinin istenmeyebileceği olaylar için toplu konuk kullanıcı hesapları oluşturmasına da izin verebilir. Çoğu zaman misafir toplu kaydı , toplu olarak uygulanan önceden onaylanmış kaydı kullanır. Çoğu durumda , her kullanıcı için API veya e-posta entegrasyonları aracılığıyla otomatikleştirilebilen benzersiz kimlik bilgileri vardır. Genelde konukların etkinlik sırasında kendi kendilerine kayıt olmalarına izin vermek veya etkinliğe özel SSID sunmak gibi daha basit ve daha kolay seçenekler vardır.

Kabul Edilebilir Kullanım Politikaları için Captive Portallar ; Captive portallar basitçe sunmak ve bir kullanıcıdan kuruluşun kabul edilebilir kullanım koşullarını kabul etmesini istemek için de kullanılabilir. Kabul edilebilir kullanım politikaları , genel olarak kullanıcının ağ üzerinde nasıl davranmasının beklendiğini ele alarak kuruluşu herhangi bir sorumluluktan muaf tutar. Bu amaç için sabit portal kullanıldığında , kayıt yöntemlerinden herhangi biri ile birleştirilebilir veya kullanıcının kabul düğmesine tıklaması için sunulabilir , sadece sayfayı sunabilir ve devam ederek kullanıcıya kabul ettiklerini söyleyebilir. Kabul edilebilir kullanım politikası oluştururken göz önünde bulundurulması gereken faaliyetler ve konular şunlardır ; Telif hakkı yasalarını ihlal eden verilerin paylaşımı veya erişimi de dahil olmak üzere yasa dışı dosya paylaşımı. Çocuk Koruma Yasasını ihlal eden içerik dahil yasa dışı içerik Telif Hakkı İhlali ve Dijital Telif Hakkı Yasası. IP bağlantı noktası taraması , DoS ve kötü amaçlı yazılım dağıtımı gibi dijital keşif ve saldırılar. İstenmeyen e-postaların (spam) gönderilmesi. Kurumun IP alanının yasal işlemle veya reddedilen listeye alınmasıyla sonuçlanabilecek herhangi bir faaliyet.

Ek olarak da kabul edilebilir kullanım politikası , hizmetlere erişim veya erişilebilirlik beklentilerini de ele almalıdır ; Kuruluş hizmetleri garanti etmez. Aktarılan verilerin şifrelenemeyeceği veya başka bir şekilde güvence altına alınamayacağına dair sorumluluk reddi. Kuruluş , kullanıcının uç noktasındaki herhangi bir hasardan veya ağın kullanımından kaynaklanabilecek herhangi bir veriden sorumlu değildir.

BYOD için Captive Portallar ; Captive portallar , uç nokta kaydı (kullanıcı kaydının aksine) ve BYOD için de kullanılır. Bu senaryolarda , portal sayfaları ve iş akışları , uç nokta kaydı ve BYOD'nin çoğunlukla yönetilen bir kullanıcıya bağlı olduğu dikkate değer istisna dışında , konuk kaydı seçeneklerine benzer görünebilir. Kurumsal ortamlarda çalışanının kişisel cep telefonunu şirketin BYOD politikası kapsamında kaydettirdiği anlamına gelebilir ve üniversite senaryosunda öğrenci yazıcısını kolejin portal sistemine MAC adresiyle kaydettirebilir. Bu durumların her birinde , kimlik doğrulama için kullanıcı kimlik bilgilerini sağlayacak ve ardından uç noktalarını kurumsal hesaplarına ekleyecektir. Bu özellik çoğunlukla çeşitli NAC ürünlerinde bulunur fakat bazı Wi-Fi ürünleri , çoğunlukla Microsoft Azure veya Google gibi bulut hizmetleri aracılığıyla yerel olarak entegre edilmiş sınırlı yeteneklere sahip olabilir.

Ödeme Ağ Geçitleri için Captive Portallar ; Konuk kayıt paketinin bir parçası olan sabit portallar , ödeme tabanlı kapılı internet erişimi için de kullanılabilir. Ağırlama ve uçaklardakiler gibi belirli noktalar , bu amaç için captive portalları kullanma eğilimindedir. Ödeme tahsilatı nedeniyle , belirli kişisel bilgilerin toplanması zorunludur. Bu nedenle sabit portal türleri , misafir kayıt modelinin bir uzantısıdır. Çoğu kurumsal ortamda yaygın olmasa da , birçok kurumsal Wi-Fi ürünü , erişim için ödeme işleme için yerel destek sunar.

Açık Güvenlik ve Gelişmiş Açık Ağlarda Güvenlik ; Endüstri artık iki açık ağ çeşidine sahiptir ; WPA2 döneminden kalma eski Açık Sistem Kimlik Doğrulama (Açık) ağları ve şifreleme sunan daha yeni Gelişmiş Açık profil.

Eski Açık Sistem Kimlik Doğrulaması (Açık) , kablosuz olarak şifreleme sunmaz.

Yeni Gelişmiş Açık , kablosuz olarak kimliği doğrulanmamış şifreleme sunar ancak kimlik doğrulaması yoktur.

Captive Portal Süreçleri için Erişim Kontrolü ; Captive portallar , kullanıcılar için amaçlanan sınırlı erişimleri nedeniyle ek güvenlik planlaması gerektirir. Sabit portallar için erişim denetimi ilkelerini yapılandırma , ürüne ve uygulamaya göre değişir. Asgari olarak sadece internet kullanımına yönelik sabit portallar , konuk kullanıcıların ağ üzerindeki üretim kaynaklarına erişmesini önlemek için katı politikalara ve segmentasyona sahip olmalıdır. Kontrollerin düzgün çalışmasını ve doğru bölümlendirmeyi sağlamak için erişim düzenli aralıklarla test edilmelidir.

Wi-Fi için LDAP Kimlik Doğrulaması ; Hemen hemen her durumda , kurumsal Wi-Fi , RADIUS aracılığıyla kullanıcı dizini deposuna karşı kimlik doğrulaması yapacaktır. Harici RADIUS sunucusu kullanmadan Microsoft Active Directory gibi LDAP dizininde doğrudan kimlik doğrulaması yapabilen bazı küçük işletme ürünleri vardır. İşte o modellerden ikisi şöyledir ; 802.1X güvenli ağların doğrudan LDAP'ye yapılandırılmasına izin veren 802.1X Ürünleri için Yerleşik RADIUS Hizmetlerine Sahip Wi-Fi , RADIUS ve EAP 802.1X'in çalışma şekli olduğundan , Wi-Fi ürünlerinde basit RADIUS sunucusunu barındırır . Bu durumda Wi-Fi altyapısı basitçe RADIUS sunucusu olarak görev yapmaktadır. LDAP'ye farklı (802.1X olmayan) bağlantılar sunan 802.1X Olmayan LDAP Kimlik Doğrulama Ürünlerine Captive Portal ile Wi-Fi , genelde kullanıcıya ürün üzerinde barındırılan ve daha sonra LDAP (RADIUS'a karşı) bağlantısına sahip olan sabit portal deneyimi sunar. 802.1X olmadığı için kimlik doğrulama EAP/RADIUS yerine LDAP olabilir. Kurumsal sınıf ürünler bu özelliği desteklemez.

Wi-Fi'de 4 Yönlü El Sıkışma ; 4 yönlü el sıkışma , 802.1X kimlik doğrulamasından sonra gelir. Bu nedenle , olayların mükemmel zihinsel zaman çizelgesinin oluşturulmasına yardımcı olur. Uç nokta ile son nokta arasında meydana gelen 4 yönlü el sıkışmanın temel işlemini anlamak önemlidir. Değiş tokuş , sorun giderme için güvenlik bağlamında ve çeşitli şifreleme anahtarlarının oluşturulma , dağıtılma biçimindeki rolü nedeniyle önemlidir.

4 Yönlü El Sıkışma İşlemi ; 4 yönlü anlaşma , hem parola korumalı hem de Enterprise / 802.1X güvenli ağlarda gerçekleşir. 4 yönlü el sıkışma sırasında uç nokta ve AP'nin her biri , kablosuz olarak iletilmeyen bilinen bir değerle başlayarak veri şifreleme için kullanılan anahtar setlerini türetmek için kullanılan giriş değerleriyle dört mesaj alışverişinde bulunurlar. 4-yollu el sıkışma , değiş tokuşlar için EAPoL (LAN üzerinden EAP) protokolünü de kullanır fakat bunun hem parola korumalı hem de 802.1X güvenli ağlar için geçerli olduğunu unutmayınız.

Genelde EAP veya EAPoL görmek , özellikle 802.1X kimlik doğrulamasından bahsettiğimiz bir tetikleyicidir. Adım adım 4 yönlü el sıkışma süreci şöyledir ; Uç nokta , AP ile ilişkilendirmeyi ve varsa 802.1X kimlik doğrulamasını tamamlamış olacaktır. Hem AP hem de uç nokta , bu süreçten ikili ana anahtar (PMK) için bilinen bir değere sahiptir. Mesaj 1'de AP , uç noktaya ANonce adlı bir değer gönderir (Authenticator Nonce , sadece kriptografik işlevlerde bir kez kullanılan , sözde rasgele oluşturulmuş bir değerdir). Akabinde uç nokta , AP ile tek noktaya yayın şifrelemede kullanılacak ikili geçiş anahtarını (PTK) hesaplamak için ihtiyaç duyduğu girdilere sahiptir. Mesaj 2'de uç nokta , AP'nin bütünlüğü doğrulaması için SNonce (uç noktanın veya talep sahibinin sahte rasgele oluşturulmuş değeri) artı mesaj bütünlüğü kontrol (MIC) değeri göndererek karşılık verir. AP daha sonra , tek noktaya yayın şifrelemesi için kullanılan ikili geçiş anahtarı (PTK) ve yayın şifrelemesi için kullanılan grup geçici anahtarı (GTK) dahil olmak üzere ilk anahtarları türetmek için gereken tüm değerlere sahip olacaktır. Bu aşamada hem uç nokta hem de AP , PTK'yı türetmiştir. Mesaj 3'te AP , mesaj bütünlüğü kontrol (MIC) parametresi ile birlikte grup geçici anahtarı (GTK) ile uç noktaya sağlayacaktır. Son olarak da mesaj 4'te uç nokta , AP'ye bir onay ile yanıt verir.

İlk değiş tokuşlardan türetilen anahtar kümeleri olduğundan , bu biraz basitleştirmedir. Çiftli geçici anahtar (PTK) , farklı amaçlar için kullanılan beş farklı anahtardan oluşurken grup geçici anahtarı (GTK) , çeşitli yayın şifreleme kullanımları için üç benzersiz anahtara sahiptir ; AP ile tek uç nokta arasındaki tek noktaya yayın trafiği için ikili anahtarlar kullanılır. Grup anahtarları , AP ile aynı BSSID'deki tüm uç noktalar arasındaki yayın ve çok noktaya yayın trafiği için kullanılır. Ana anahtarlar hiyerarşinin en üstündedir , değişmezdir ve anahtar türetme zinciri için kullanılır. Geçici anahtarlar , diğer anahtarları türetmek için kullanılır. Verileri şifrelemek için geçici anahtarlar kullanılır.

WPA2-Kişisel / WPA3-Kişisel ile 4 Yönlü El Sıkışma ; WPA2-Kişisel parola tabanlı SSID'lerde el sıkışma , tüm uç noktaların bir AP'ye bağlanmak için her yerde kullanılan yöntem olan Açık Sistem Kimlik Doğrulaması ve ilişkilendirme sürecinden hemen sonra gerçekleşir. WPA3-Kişisel SSID'lerde , SAE süreci , ilişkilendirme isteğine ve yanıtına geçmeden önce SAE-Kimlik Doğrulama taahhüdünü , değişimleri onaylamayı içerir. Bu değiş tokuşlar sırasında ikili ana anahtar (PMK) türetilir. SAE'li WPA3-Kişisel'de şifreleme anahtarı türetme parolanın uzunluğunun bir fonksiyonu değildir. PSK'lı WPA2-Kişisel'de veri şifreleme anahtarları doğrudan paroladan türetilir. WPA3-Personal'ın eski muadilinden çok daha güvenli olmasının nedenlerinden biridir.

WPA2-Enterprise ve WPA3-Enterprise ile 4 Yönlü El Sıkışma ; 802.1X güvenli ağlarda (WPA2-Kuruluş veya WPA3-Kuruluş) el sıkışma , uç nokta başarılı EAP kimlik doğrulamasını tamamladıktan sonra gerçekleşir. 4 yönlü el sıkışma Wi-Fi'de çok temel ve yaygın işlem olduğundan , işleyişini anlamak , ağ tabanlı kimlik doğrulama dışında gelişmiş sorun giderme için yararlı bir bilgidir. Kimlik doğrulama 802.1X Kontrolsüz Bağlantı Noktasında gerçekleşerek uç noktanın kimliği doğrulandıktan sonra , 4 yönlü anlaşma şimdi açılan Kontrollü Bağlantı Noktasında devam edebilir.