

AAA Güvenlik Konsepti

Daha önceden Safa Kısıklılar Layer 2 Güvenlik Yöntemleri (Bölüm 1) yazısında daha çok cisco cihazlar üzerindeki yapılandırma ve örneklerden bahsetmişti. Ben de bu yazımda Safa arkadaşımızın yazmış olduđu bu dökümandaki bazı terimleri biraz daha genişçe almak istedim.

Authentication (dođrulama), Authorization (yetkilendirme) ve Accounting (aktivite izlenmesi) kısaca AAA olarak bilinen ve ađ kaynaklarına güvenli erişimi sađlayan güvenlik unsurlarıdır. AAA servislerine ulaşabilmek için iki tip erişim metodu vardır:

- **Karakter modu:** Yönlendiriciye, yönetim amaçlı gönderilen isteklerdir.
- **Paket modu:** Başka bir ađda bulunan cihaza erişim için gönderilen isteklerdir.

AAA güvenlik unsurlarına bankaların uyguladıđı kredi kartı sistemi örnek olarak verilebilir. Bankanın kullanıcıya vermiş olduđu kartın üzerindeki kart numarası, ad, soyad ve son kullanma tarihi bilgileriyle dođrulama işlemi gerçekleştirilir. O kullanıcıya verilmiş olan harcama limiti ile yetkilendirme işlemi yapılır. Nerede, ne zaman, ne kadar harcama yaptıđının kayıt altına alınması ve sonucunda bir ekstre oluşturulması ile de kullanıcı aktivitelerinin izlenmesi işlemi yapılır.

Authentication (Dođrulama):

Kullanıcının sisteme bağlanabilmesi için ilk başta yapılması gereken işleme **authentication (dođrulama)** denir. Ana bilgisayar, anahtarlayıcı veya yönlendirici kullanımı sırasında cihaz veya kullanıcının kimliđinin dođrulama işlemidir. Bu işlem ile kullanıcının sahip olduđu kullanıcı adının sistemde kayıtlı olup olmadığı kontrol edilir. Daha sonra kullanıcıya verilen parola da kontrol edilerek dođrulama işlemi yapılır. Dođrulama sađlanırsa kullanıcıya sisteme giriş izni verilir. Sistem üzerinde açık bulunan her port ve servis göz önünde bulundurularak sisteme anonim erişim verilebilir. Şifrelerin gerektiđi kadar güvenli olabilmesi de uygulanmakta olan şifre politikasına bađlıdır.

Dođrulama işlemi iki şekilde yapılır:

- **Yerel AAA Dođrulaması:** Yönlendiricinin kendi veritabanımında bulunan kullanıcı adı ve şifreleriyle yapılır. Genellikle küçük ađlarda uygulanır.
- **Sunucu-Tabanlı AAA Dođrulaması:** Eđer ađda bulunan yönlendiricinin miktarı fazla ise sunucu-tabanlı AAA dođrulaması uygulanır. Sistemde kullanılan kullanıcı adı ve şifreler bu sunucuda saklanır ve dođrulama işlemi sunucuda yapılır.

Authorization (Yetkilendirme)

Kullanıcı adı ve şifre dođrulaması sađlanan kullanıcıların sisteme, programa veya ađa hangi yetkilerle erişim hakkına sahip olduklarını belirten sisteme **authorization (yetkilendirme)** denir. Sisteme kayıtlı olan kullanıcılar gruplanarak, bu gruplara çeşitli yetkiler verilir. Kullanıcı içerisinde bulunduđu grubun bütün yetkilerine sahiptir. Eđer bir kullanıcı birden fazla gruba üye ise bu gruplara verilen yetkilerin hepsine sahiptir. Güvenliđin tam olarak sađlanabilmesi için kullanıcılara gerekenden fazla yetki verilmemelidir. Yetkiler verilirken sistem üzerindeki açık her bağlantı noktası (port) göz önünde bulundurulmalıdır.

Accounting (Aktivite İzlenmesi)

Bir sorun ile karşılaşıldığında sorunun tespitinin sağlanabilmesi için kullanılan sisteme **accounting (aktivite izlenmesi)** denir. Sistemde bulunan kullanıcıların yaptıkları bütün işlemler ve erişim saatleri kayıt altına alınır. Bir problem çıktığında ise kullanıcı aktivitelerinin tutulduğu bu kayıtlardan sorun anlaşılmasına ve çözülmeye çalışılır.

RADIUS

RADIUS, Remote Authentication Dial In User Service (Uzaktan Aramalı Kullanıcı Kimlik Kanıtlama Servisi) uzaktan ağa erişmek isteyen kullanıcıların kimlik denetimini gerçekleştirmek üzere IETF (Internet Engineering Task Force) tarafından standartlaştırılan bir protokoldür. İlk başta internet servis sağlayıcıları, ağını kullanmak isteyen kullanıcıların kullanıcı adı ve parola doğrulamasının sağlanması için kullanılmıştır. RADIUS iletim için UDP (User Datagram Protocol) kullanır. Bu protokol İnternet erişimi ve elektronik posta servisi erişimi yanında RAS (Remote Access Server- Uzak Erişim Sunucusu) ve VPN (Virtual Private Network - Sanal Özel Ağ) gibi sistemlerde sıklıkla kullanılır. Bu protokol ile kaynaklara güvenli erişim için gereken güvenlik unsurları yani doğrulama, yetkilendirme ve kullanıcı aktivitelerinin izlenmesi sağlanır. Bir istemci ağa erişmek istediğinde sunucu üzerinden ağa erişmek için RADIUS sunucusuna istek gönderir. RADIUS sunucusu 3 farklı biçimde bu isteğe cevap verebilir:

- **Access Reject (Erişim reddi):** Kullanıcı doğrulama işlemi gerçekleştirilemez ve RADIUS sunucusu, kullanıcıya ağ kaynaklarına erişemeyeceği konusunda bu cevabı gönderir.
- **Access Challenge (Erişim Kimlik Sorgusu):** RADIUS sunucusu kullanıcıya ağa erişebilmesi için ikinci bir şifre isteyen bir cevap gönderir.
- **Access Accept (Erişim Kabulü):** Kullanıcıların bilgileri doğrulanır ve RADIUS sunucusu kullanıcının ağa erişimine izin verir.

Bu protokolün örneklerinden biri de FreeRADIUS adına sahip açık kaynak kodlu ve günümüzde bütün kimlik yetkilendirme protokolleri ve veritabanlarını destekleyen bir yazılımdır. Bu yazılım ile yapılabilecek işlemler:

- Ağa erişmek isteyen kişiler için doğrulama işlemi yapılır.
- Ağa erişebilen bütün kullanıcılar için ayrı ayrı yetkilendirme yapılabileceği gibi kullanıcılar gruplanıp, gruplara yetkiler verilebilir.
- Sisteme o an içinde bağlı olan kullanıcılar gözlemlenebilir.
- Proxy kullanımını destekler.