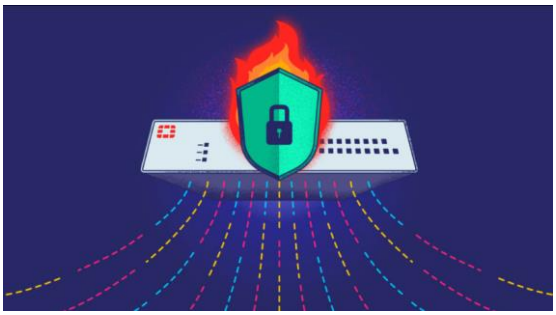

FORTIGATE SSL VPN SIKILAŞTIRMA

Aşağıda belirtilen uygulamaları gerçekleştirerek Fortigate cihazınızda ki SSL VPN'inize sızmayı önemli ölçüde zorlaştırabilirsiniz.

Varsayılan SSL VPN bağlantı noktası 443/10443'ü değiştirme ; 443 ve 10443 portları , iyi bilinen Fortigate dinleme bağlantı noktalarıdır. En başta yapmamız gereken sıkılaştırma bu portları değiştirmektir.

CLI'da girilecek komut:

config vpn ssl settings

set port 14324

Kimlik doğrulama için yerel " local " kullanıcıları kullanmayınız ; Lokal kullanıcıları kimlik doğrulama için kullanmayınız. Eğer kullanmak durumundaysanız şifreleri başka yerde saklayın veya MFA'yı etkinleştiriniz. Tüm güvenlik bilgilerini tek bir cihazda tutmak kötü bir uygulamadır. CVE-2018-13379 güvenlik açığı sadece yerel kimlik doğrulamasına sahip yerel VPN kullanıcıları bulunan Fortigate cihazlarını etkilemişti. Kullanıcı kimlik doğrulamasını mevcut kullanıcı veritabanıyla entegre etmek Fortigate cihazında kolaydır.

VPN kullanıcıları için Çok Faktörlü Kimlik Doğrulamayı etkinleştiriniz ; MFA , bizler için iyi bir sıkılaştırma olacaktır. Fortigate cihazı ücretsiz olarak 2 mobil uygulama FortiToken ile birlikte gelir. Ayrıca SMS'i MFA olarak kullanabilirsiniz fakat maliyet çıkaracaktır. MFA sağlayan 3. taraf RADIUS protokolü aracılığıyla kullanılabilir. Oldukça güvenli olan fakat aynı zamanda kurulumu en karmaşık olan MFA olarak istemci PKI sertifikaları seçeneği de bulunmaktadır. İstemci sertifikaları SAML kimlik doğrulamasıyla (Azure ve benzeri) birlikte çalışmaz. Sonuçta bu da bir dezavantajdır.

VPN SSL portalına erişimi belirli IP adresleriyle sınırlayınız ; Kullanıcılarınızın İSS'leri tarafından atanan statik IP adresleri varsa , VPN SSL portalının maruz kalmasını sınırlamanın mükemmel bir yoludur.

VPN SSL dinleme arayüzünü Geri Döngü arayüzüne " Loopback Interface " taşıyınız ; Güvenlik kurallarında ek güvenlik kontrolü sağlayacaktır. Faydaları ; Kural oldukça görünürdür. CLI'de Yerel İlke olarak gizlenmez. Ayrıntılı trafik ve güvenlik günlüklerine sahip olacaktır. SSL VPN erişiminin belirli bir zaman planına göre açılıp kapatılmasını sağlar. Hiçbir şeyi silmeden tek tıklamayla SSL VPN erişimini devre dışı bırakmamıza olanak tanır. ISDB adres nesnelerinin kullanılmasını mümkün kılar. SSL VPN , Fortigate'te donanım hızlandırmalı olmadığı için fiziksel veya Loopback arayüzünde nerede ayarlanmış olursa olsun , burada Loopback'ten kaçınmak için hiçbir neden bulunmamaktadır.

Ayarlamak için ; Geri Döngü arayüzü oluşturun. VPN SSL Ayarlarında bu Geri Döngüde VPN SSL'yi etkinleştiriniz. İnternetten dinleme bağlantı noktasındaki Geri Döngüye erişime izin veriniz. FortiOS 7.2'den başlayarak , Yerel Politikalarda GeoIP nesnelerini , harici beslemeleri de kullanabiliriz. Yerel Giriş Politikasının sadece CLI doğası nedeniyle , SSL VPN bağlantıları için Loopback kullanmak daha kolay yönetilebilir. Ancak Yerel giriş politikası da bu işi yapabilir.

GeoIP konumuna göre portala erişimi sınırlayınız; Kullanıcılarınız belirli bir ülkede veyahut ülkelerde bulunuyorsa , VPN erişimini en azından bu ülkelerle sınırlamanız önerilir. Coğrafya türünde adres oluşturup , VPN SSL Ayarlarında kullanınız.

Tor Çıkış Relay ve Node " Düğümlerinden " herhangi erişimi engelleyiniz; Tor kullanan saldırganların takibi neredeyse imkansızdır. Bundan dolayı Tor ağından kaba kuvvet saldırıları yaygın olarak yapılır. Sadece SSL VPN'iniz Loopback arayüzünü dinlerken uygulama yapmak mümkündür. Bunları engellemek için Tor Çıkış Düğümleri ve Relay'leri için ISDB nesnelerini ve VPN SSL kuralının üzerindeki güvenlik kuralındaki VPN Anonimleştiricilerini kullanmanız yeterlidir.

CA tarafından verilen güvenilen sertifikayı yükleyiniz ; Yükleyebilirsiniz fakat Let's Encrypt sertifikalarını doğrudan Fortigate üzerinde yayınlamayınız. VPN SSL'ye her girişte güvenilir CA Yetkilisinden alınan geçerli TLS sertifikası ortadaki adam saldırısına maruz kaldığında tarayıcı hatasını hemen yakalayacakdır.

Sertifikaları şifreleyebilirsiniz fakat bunları doğrudan Fortigate'te yayınlamanın bazı dezavantajları vardır ;

a. Acme protokol arka plan programının 80 numaralı bağlantı noktasını dinlemesini sağlayarak otomatik yenilemenin çalışması için herhangi bir noktadan açık olması zorunludur. Herhangi ek arka plan programının İnternet'e açık hale getirilmesi kötü bir fikirdir. 80 numaralı bağlantı noktasını yalnızca sertifikanın verildiği / yenilendiği süre boyunca açık tutmanız gerekir.

Bu nedenle de isterseniz sertifika talep ederken herhangi bir yerden gelen 80 numaralı bağlantı noktasını etkinleştirebilir ardından yenileme zamanı gelene kadar bağlantı noktasını kapatabilirsiniz. Ancak manuel olarak talep edip içe aktarmaktan hiçbir farkı yoktur.

b. Joker karakter sertifikalarının istenmesini desteklemez. Belirli alt alan adını destekler. Dezavantajı ; VPN alt alan adınız internette herkesin görebileceği şekilde oturum açar.

Her başarılı VPN SSL bağlantısında e-posta uyarısını yapılandırınız; Çoğu kişi için başarılı giriş , başarısız girişten daha önemlidir.

Paralel olarak bağlanmak için aynı kullanıcı hesabının yeniden kullanılmasını önleyiniz; Varsayılan olarak aynı VPN kullanıcısına farklı konumlardan aynı anda bağlanabilirsiniz. Bunu iyileştirmek için kullanıcılar için eşzamanlı oturum açmayı devre dışı bırakınız.

CLI'da yapılandırma komutu:

```
config vpn ssl web portal
  edit "full-access"
  set limit-user-logins enable
end
```

Güvenlik kurallarında , tümüne değil , sadece belirli hedeflere ve hizmetlere erişime izin veriniz. Yöneticiler , SSL VPN güvenlik kuralının Hedef sütununa belirli hizmetlere sahip belirli host bilgisayarlar yerine tüm LAN'ı eklerler. Saldırganlar Fortigate'e VPN bağlantısını ele geçirirse, AD Etki Alanı Denetleyicileri ve SMB paylaşımları için dahili LAN'ı toplu olarak tarayabilir, tüm host bilgisayarları numaralandırabilecektir. VPN Uzaktan Erişim kurallarını belirli hizmetlere ve host bilgisayarlara sıkılaştırırsanız bunların hiçbiri gerçekleşmeyecektir.

VPN SSL kullanmıyorsanız devre dışı bırakınız veya boş arayüze atayınız; VPN SSL ayarı varsayılan olarak açıktır ve bunda herhangi bir sorun yoktur. Kendisine atanmış dinleme arayüzü olmadığı ve ssl.root kullanan güvenlik kuralı bulunmadığı sürece hizmet dinlenemez. Bazı FortiOS sürümlerinde bunu CLI'de yapmanız gerekir. Hiçbir şeyi silmeden SSL VPN'yi geçici olarak devre dışı bırakmak istiyorsanız , Devre Dışı Bırak'a tıklamanın yanı sıra, ona yine Aşağı durumuna koyacağınız Geri Döngü arayüzü atayabilirsiniz.

CLI yapılandırması:

```
config vpn ssl settings
set status disable
  set source-interface Loop1
end
```

N sayıda başarısız denemeden sonra istek yapan IP'yi engelleyiniz; Böylelikle VPN SSL'ye yönelik kaba kuvvet ve tarama saldırılarını yavaşlatır. Bu özellik varsayılan olarak açıktır ancak engelleme süresi yalnızca 60 saniyedir. Bunu ortamınıza ve kullanıcılarınıza göre ayarları özelleştirebilirsiniz.

CLI'de yapılandırılabilirsiniz:

```
config vpn ssl settings
  set login-attempt-limit 5
set login-block-time 700
end
```

SSL VPN için zayıf ve güncel olmayan TLS protokollerini devre dışı bırakınız ; Yeni FortiOS sürümlerinde bile VPN SSL , varsayılan olarak güncel olmayan ve her yerde kullanılması tavsiye edilmeyen TLS 1.1 ve TLS 1.2 sürümlerini destekler. Bu komutla SSL VPN'i yalnızca TLS 1.2 ve 1.3 (yalnızca CLI'de) kullanacak şekilde ayarlayabilirsiniz.

```
config vpn ssl settings
set ssl-min-proto-ver tls1-2
end
```

Bu komutla eski tarayıcıların ve eski Forticlient'ların bağlanmasını engelleyecektir.

İstemciler için VPN SSL'den VPN IPSec'e geçiş yapmayı düşününüz; Daha fazla efor isteyebilir ama karşılığını alacaksınız. İstemci tarafında aynı Forticlient'i kullanırsınız.