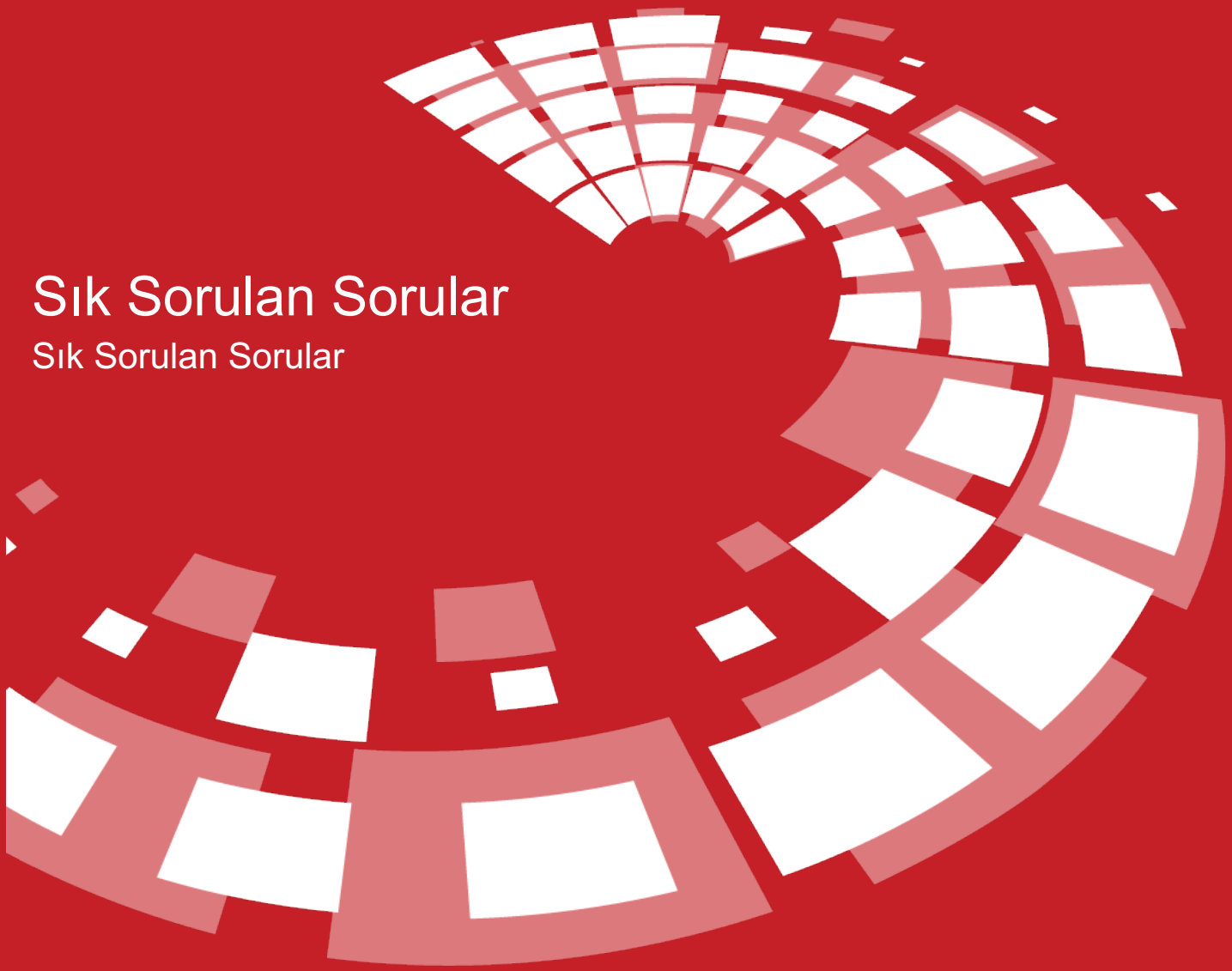
epati
BİLİŞİM TEKNOLOJİLERİ

Sık Sorulan Sorular

Sık Sorulan Sorular



www.epati.com.tr

Sık Sorulan Sorular

Antikor kurulumunu nasıl yapabilirim ?

> Antikor NGFW Kurulum Kılavuzu ve Antikor Layer 2 Tünel Kurulum Kılavuzuna linklerine bakarak kurulumunuzu kolayca yapabilirsiniz.

Mevcut lisans ile kaç kurulum yapabilirim ?

> Mevcut lisans ile **aynı makineye** maksimum 10 kez kurulum yapılabilmektedir. Kurulum hakkına ihtiyaç duyulması halinde teknik@epati.com.tr e-posta adresi ile iletişime geçebilirsiniz.

Lisansımın kapsamına nereden bakabilirim ?

> Antikor web arayüzü açıldığında sağ üst köşede, *Çıkış Yap* seçeninin hemen yanındaki kart simgesine tıklayarak; lisans içeriğinizi ve sürüm listenizi görebilirsiniz.

Arayüze erişemiyorum, erişimi nasıl açabilirim ?

> Cihazınıza klavye ve monitör bağlayarak Konsol ekranına kullanıcı adı: admin, parola: antikor ile eriştikten sonra; Sistem Ayarlarından, Yönetim Paneli Erişim Ayarlarına girilir ve yeni kayıt ekleme sihirbazı ile erişilecek IP adresi eklenmelidir.

Arayüz kullanıcı adımı veya şifresini unuttum. Parola sıfırlama nasıl yapabilirim ?

> Cihazınıza klavye ve monitör bağlayarak Konsol ekranına kullanıcı adı: admin, parola: antikor ile eriştikten sonra; Sistem Ayarlarından, Kullanıcı Şifresini Değiştir'e girip kullanıcıları listeleyip, şifrenizi değiştirebilirsiniz.

Antikor NGFW'ye ağdan erişemiyorum, IP adresini nasıl değiştirebilirim ?

> Cihazınıza klavye ve monitör bağlayarak Konsol ekranına kullanıcı adı: admin, parola: antikor ile eriştikten sonra; Network IP Ayarlarından, WAN Ayarlarına girip kullanıcıları listeleyip, IP adresinizi değiştirebilirsiniz.

SSH bağlantısı nasıl sağlarım ?

> Kullanıcılar öncelikle ssh-key üretip bunu Antikor'a tanıtmalıdır. Kullanıcı SSH Yapılandırma örneği bu konuda sizlere yardımcı olacaktır. Ürettiğiniz ve Antikor'a tanıttığınız ssh key'i kullanarak, ürününüzün IP adresi ile 22022 portundan erişim sağlayabilirsiniz.

Kurulum sonrasında donanım değiştirebilir miyim ?

> Antikor ürünleri kurulum esnasında donanımı algılar ve donanımınıza göre kurulum sağlar. Kurulum sonrasında donanım değişikliği yapılmamalıdır.

Nasıl Statik NAT yapabilirim ?

> Statik NAT Yapılandırma örneği bu sorunuza çözüm sağlayacaktır.

Active Directory Entegrasyonu nasıl yapabilirim ?

> Active Directory ve Antikor tarafında yapmanız gerekenler adım adım Active Directory - Kerberos SSO Entegrasyonu yapılandırma örneğinde anlatılmıştır.

Antikoru Yönetirken Kurumdaki diğer sorumlu arkadaşlara Network ve Menü Tabanlı Yetkilendirme yapabilir miyim ?

> Antikor NGFW, yetkilendirme yaparken ağ grubuna göre de yetkilendirme yapabilmektedir. Her ağın yönetimini farklı kullanıcılara yetkilendirebilir, iş yükünüzü paylaşabilirsiniz. Yöneticiler, sadece yetkili oldukları ağlara dair ayarları görüp, yönetebilirler. Detaylı bilgi için Yönetim Paneli Kullanıcıları dokümanına göz atabilirsiniz.

Antikor nereye konumlandırılmalıdır, internet bağlantı türü olarak hangilerini destekler ?

> Antikor gelen internet bağlantısının hemen önüne konumlandırılır. Çalışma modu olarak xDSL ler için PPPoE modunu, Metro ethernet ve Routerlar için Routing modunu destekler. Ağında hiçbir değişiklik yapmak istemeyenler için de Transparent (Bridge) modunu destekler.

Antikor'un Cluster Desteği var mıdır ?

> Evet vardır. Sistemin yedekli çalışmasını destekleyen özelliktir. Sürekliliğin sağlanabilmesi amacıyla geliştirilen Antikor'ların eş zamanlı ve ortak çalışması temeli üstüne kuruludur. Clusterdaki bir sunucunun donanım ya da yazılım problemi oluştuğunda diğer bir sunucunun otomatik olarak devreye girmesi sağlanmaktadır. Böylece süreklilik sağlanmış olur. Detaylı bilgi için Cluster Ayarları dokümanına ve Cluster yapılandırma örneğine göz atabilirsiniz.

Antikora gelen yenilikler veya güncellemeler nasıl yüklenir ?

> Antikorda Otomatik Güncelleme Sistemi vardır. Antikor NGFW'nin otomatik güncelleme sistemi ile yeni güncelleştirmeler online olarak kontrol edilir. "Güncellemeye Hazır" şeklinde Paketler tek tek listelenir. Kullanıcı "Güncelleştirmeye Başla" deyince güncelleme yapılır. Güncelleme kritik ise kırmızı bir şekilde "Kritik" ibaresi butonda yer alır. Veritabanları "Otomatik" güncellenir. Tüm paketler önceki versiyona geri alınabilir.

Yerel ağımdaki kullanıcıların bilgilerini nasıl doğrularım ?

> Antikorda yerel ağınıza katılmak isteyen her istemci, Antikor NGFW Kayıt Servisi formu ile karşılanır. Burada TC Kimlik numarası doğruluğunun kontrolü vardır. Geri planda kullanıcının MAC ve IP bilgisi de otomatik alınır. Formda alınan kimlik bilgileri KPS(MERNİS) üzerinden doğrulandığı gibi SMS, LDAP, RADIUS, POP3 doğrulaması da yapılabilmektedir. Detaylı bilgi için Kayıt Servisi Yapılandırma örneğine göz atabilirsiniz.

Yerel ağımda enfekte olmuş bilgisayarları nasıl engellerim ?

> Antikor NGFW AntiBot Modülü, ağınızdaki enfekte olmuş bilgisayarların BotNet'lere hizmet etmemesi için botnet komuta sunucuları ile iletişimi keser. Detaylı bilgi için Ağ tanımları dokümanına göz atabilirsiniz.

Antikor yerel ağımda olmayan IP adreslerine tarama yapanlara karşı nasıl önlem alır ?

> Antikor NGFW kendi IP havuzunda olmayan ve kendine gelen IP leri Karadelik Servisine gönderir. Bu paketler yönlendirilmez ve göz ardı edilir.

Antikor tanımlı olmayan IP adreslerinden gelen trafiği geçirir mi ?

> - Kurum içerisindeki bütün kullanıcılardan gelen trafiği analiz ederek, IP Spoofing adıyla bilinen IP

aldatmaca saldırılarından ağı korumalıdır.

- AntiSpoof servisi, ağın iletişim haritasını çıkararak ağ kapsamı dışındaki IP trafiğini otomatik olarak engelleyebilmektedir.
- Kirli trafiğin ağın dışına çıkmasını engelleyebilmekte ve balküplerine yakalanmasını önlemektedir.

Ağımda hem IPv4 hem de IPv6 IP adresleri var. Aynı anda çalışır mı ?

Antikorda Dual Stack yani hem IPv6 hem de IPv4 her iki protokol da aynı anda çalışır. Aynı anda hem IPv4 hem IPv6 üzerinden trafik denetimi ve analizi sağlar.

Antikor hangi katmanlarda koruma sağlar ?

Antikor Dual Layer - Çift katman aynı anda çalışır. Hem Layer2 hem Layer 3 haberleşmenin avantajlarından aynı anda faydalanabilirsiniz.Antikor NGFW, VLAN'larınızla hem Layer2 haberleşip MAC adreslerini toplayabilir, anormallikleri tespit edebilir, hem de direk bağlı ağlarınızda dahi Layer3+ ve üstü yönlendirme yapabilirsiniz.

SYN ataklarına karşı bir koruma var mıdır ?

Antikorda SynFlood koruması vardır. Hem yerel ağdan hemde internetten gelen SYN ataklarına karşı korur. İstenilen IP ve portlar bu sistemden hariç tutulabilir.

Antikorda internet trafiğinde araya sızan trafikler nasıl önlenmektedir ?

Antikorda SPI – Statefull Packet Inspection (Durumsal Paket Analizi) modülü vardır. Paketlerinizin başlangıcından itibaren hangi aşamada olduğunu takip eder. Takip edilen her bağlantı, state tablosunda saklanır. Araya sızmaları ve isteği yapılmamış cevapları engelleyerek güvenliğinizi bir üst kademeye taşır.

Yerel ağımdaki kullanıcılara ayrı bant genişliği uygulayabilir miyim ?

Antikorda QoS - Etkin Bant Genişliği Yönetimi vardır. Kişi bazlı maksimum bant genişliği tanımlanabilir. Hız Garanti etme, Öncelik Atama, Kural Tabanlı QoS Uygulama, Her Ethernet Arayüzü için Farklı Yapılandırma imkanı vardır. Detaylı bilgi için Ethernet QoS ve Ethernet QoS Kuralları dokümanına göz atabilirsiniz.

Antikorda internetten networkler tanımlayıp bunları engelleyebilir miyim ?

Antikor Ağ Grupları oluşturup, bu gruplara IP adresi veya network tanımlanabilir. Bu tanımlar güvenlik kurallarında erişim izinlerinde ve özel kullanıcılar bölümünde de kullanılabilir. Ağ grubu üyeleri internetten otomatik olarak da çekebilmektedir. (Örneğin hazır IP listeleri veya URL listeleri) Detaylı bilgi için Ağ Tanımları dokümanına göz atabilirsiniz.

Antikorda Port grupları tanımlayabilir miyim ?

Antikor içinde Port Tanımları(Grup) yapılıp 140 farklı protokolde port tanımlanabilir. Bu tanımlar Güvenlik Duvarında kullanılır. Detaylı bilgi için Port Tanımları dokümanına göz atabilirsiniz.

Antikorda yerel ağımdaki istemcileri gruplayıp, bu gruplara kurallar tanımlayabilir miyim ?

İstemciler için kapsam belirtilip grup oluşturulabilmektedir. Oluşturulan gruplara tabi kullanıcıların grubunun kayıt formunda gösterilip, gösterilmeyeceği de buradan ayarlanmaktadır. Bu gruplara filtrelemelerde gerekli işlemler yapılabilir. Detaylı bilgi için İstemci Grupları dokümanına göz atabilirsiniz.

Antikorda kendi kullanıcılarıma farklı filtrelemeler yapabilir miyim ?

Antikorda hangi kullanıcı ve bilgisayarların ne türlü yetkilere sahip olacağı atamaları yapılır. Filtrelemeler de bu istemcilere atandığı biçimde çalışır. Detaylı bilgi için Özel kullanıcılar dokümanına göz atablirsiniz.

Antikorda ethernetlerin ve altında oluşturduğum VLAN'ların grafiklerini nasıl görebilirim ?

Antikorda Yerleşke ayarlarında üzerindeki bütün Ethernet, VLAN'ların trafik ve istemici sayısı bazlı RRD grafiklerini çizer. Kullanıcılar istedikleri takdirde bu grafikleri ".rrd" formatında indirebilmektedir. Oluşturulan grafikler günlük, haftalık, aylık ve yıllık olarak tutar. Detaylı bilgi için Yerleşke Ayarları dokümanına göz atabilirsiniz.

Antikorda kimlik doğrulama yapabilir miyim ?

Antikorda RADIUS servisi sayesinde kimlik doğrulama işlemleri yapılabilmektedir. Antikor kullanıcıların AAA (Authentication, Authorization, Accounting) (kimlik denetimi), yetkilendirme ve kayıt altına alma işlemleri yapabilmeleri sağlanmaktadır. RADIUS Profilleri, NAS Tanımları, RADIUS Proxy Havuzları ve Proxy Etki Alanları ile ilgili gereken ayarlamalar buradan yapılmaktadır. Detaylı bilgi için RADIUS Ayarları dokümanına göz atabilirsiniz.

Evden Kurumun üye olduğu online veritabanlarına nasıl bağlanırım ?

Proxy servisi sayesinde evden de işyerindeymiş gibi kurumun üyeliği bulunan sitelere ve üyeliklere girilebilir. Ayrıca kullanıcıların Web Filtreleme Yönetimi bölümünde tanımlanan politikalara dahil olup olmayacağı da seçilebilir. Evden giren kullanıcıların logları da tutulur. Detaylı bilgi için İstemci Tarafında Proxy Yapılandırma Örneğine göz atabilirsiniz.

Antikor hangi logları ve ne formatta tutar ?

Antikorda 24 farklı log çeşidi ve 7 farklı log formatını desteklemektedir. Sunucu sistem loglarının kayıt edileceği syslog sunucu/sunucularının ayarları yapılır, tercih edilen ham veya yapısal log formatında log toplayıcınıza veya SIEM'e iletilir. Detaylı bilgi için Syslog Ayarları dokümanına göz atabilirsiniz.

Kurumun sertifikasını Antikora tanımlayabilir miyim ?

Antikorda SSL Sertifikası Yönetimi menüsü, kurumun SSL sertifikasının tanımlandığı bölümdür. Kendi sertifikanızı oluşturabileceğiniz gibi mevcut sertifikanızı da aynı modülü kullanarak yükleyebilirsiniz. Detaylı bilgi için SSL Sertifikası Yönetimi dokümanına göz atabilirsiniz.

Kurumun tek IP adresi var ama birden fazla sunucum var, alan adına göre bu sunuculara dağıtabilir miyim ?

Http(s) Sunucu Yönlendirme Bir kurumda aynı WAN(gerçek) IP adresini kullanan ve kullandığı IP adresleriyle kurum içindeki veya dışındaki kişilere hizmet veren network bileşenlerinde erişim problemini ortadan kaldırmak için gerekli yönlendirmelerin yapıldığı modüldür. Detaylı bilgi için HTTP(S) Sunucu Yönlendirme dokümanına göz atabilirsiniz.

IP-MAC eşlemesi yapabilir miyim ?

Antikorda DHCP sayesinde cihazlara özel bir IP atama işlemi yapar. Kayıt servisi sırasında otomatik olarak IP-MAC ikilisin bağlar ve o kullanıcıyla eşleştirir.Servislerden IP-MAC eşleşmesi açıldığında IP sini değiştirenler internete çıkamaz. Detaylı bilgi için DHCP Ayarları dokümanına göz atabilirsiniz.

Antikorda tüm portların trafiğini loglayabilir miyim ?

Antikordaki Netflow Servisi, trafik bilgilerinin içeriğini değil, başlık(IP ve TCP/UDP header) bilgilerini tutabilir ve bu bilgileri bir toplayıcı(collector)'ya yollayabilir. Bu bilgileri gönderirken istenirse bütün bilgileri,

istenirse sadece bir IP'yi, istenirse de bir network grubunu toplayıcıya gönderebilir. Detaylı bilgi için Netflow Ayarları dokümanına göz atabilirsiniz.

Antikor kaç farklı dil destekler ?

Antikor'da dil ayarlarının yapıldığı alandır. Toplamda 3 adet dil seçeneği (Türkçe, İngilizce, Arapça) bulunmaktadır. Farklı web arayüz işlemleri için (örneğin kullanıcı kaydı, duyuru ekranı, erişim engel sayfası, vb.) farklı dil seçenekleri ile çalışabilmektedir. Detaylı bilgi için Dil Ayarları dokümanına göz atabilirsiniz.

Antikorun takılı olduğu switchlerden port isimlerini alabilir miyim ?

LLDP bağlantısı için ayarlar bu menüde yapılmaktadır.Ayarlar LLDP yapılacak Network'ün, sistem adı ve açıklamasının girilmesi ile tamamlanmaktadır. Gerekli ayarlar yapıldıktan sonra Anlık Gözlem menüsü altında bulunan LLDP Durumundan gözlem yapılabilmektedir. Detaylı bilgi için LLDP Ayarları dokümanına göz atabilirsiniz.

Sahip olunmayan WAN IP adreslerinin kullanılması mümkün müdür ?

Antikorda IP Havuzları bölümüne yönetmekte olduğunuz ağın IP aralıklarını (iç ve dış) tanımlamamız gerekmektedir. Bu aralıklar, Antikor'un denetleme mekanizmalarında kullanılacaktır. Eklenen VLAN IP adreslerini kendi otomatik getirir. Bazı işlemler (İstemci Tanımları, Statik NAT, vb.) IP havuzlarına IP adreslerini eklemeden yapılamamaktadır. Detaylı bilgi için IP Havuzları dokümanına göz atınız.

Ethernetlere birden fazla VLAN veya IP Adresi Atanabilir mi?

Antikorda Ethernet ayarlarından, ethernetlere (LAN), İnternete Çıkış (WAN), Sunucu Bölgesi (DMZ) ve PPPoE ayarları bu bölümden yapılır. Lisans içeriğine göre birden çok LAN, WAN ve DMZ arayüzü eklenebilir. Antikor'da IP Atama kısmından da farklı veya aynı ethernet arayüzlerine birden fazla IP adresi verilmesi gerekirse bu bölümden verilebilmektedir. Detaylı bilgi için IP Atama, Ethernet Atama dokümanlarına ve VLAN Yapılandırması örneğine göz atabilirsiniz.

Antikor Link Birleştirme türlerinden hangilerini destekler ?

Antikor'un üstünden geçen hızı artırmak veya Cluster olarak Antikor çalıştırmak için kullanılmaktadır. Birleştirme türü olarak 6 farklı seçenek mevcuttur.

- Köprüleme
- Köprüleme - Rapid STP
- Failover
- Load Balance (FEC)
- LACP
- Round Robin

Detaylı bilgi için Sanal Ethernet Birleştirme dokümanına göz atabilirsiniz.

Antikorda Ethernet üzerinde QoS yapılabilir mi ?

Ethernet paketlerinin (ses, video vb.) öncelik sırasının belirlenmesi için kullanılmaktadır. QoS uygulamalarında asıl amaç var olan bant genişliğini (bandwidth) en verimli şekilde kullanabilmesine imkan sağlamaktır. 3 farklı QOS (Quality Of Service) türü tanımlanabilmektedir: QFQ (Quick Fair Queueing), CBQ (Class Based Queueing), HFSC (Hierarchical Fair-Service Curve). Detaylı bilgi için Ethernet QoS dokümanına göz atabilirsiniz.

Antikorda yerel kullanıcılara duyurularımı nasıl iletirim ?

Ağınızdaki tüm kullanıcılara, gruplara, IP veya IP bloklarına duyuru yapabilirsiniz. Duyuru yaptığınız kişiler hangi sayfaya girerse girsin yapılan duyuru karşısına çıkmaktadır. Okudum tuşuna basılmadığı sürece internete çıkmaya devam edemez. Detaylı bilgi için Duyuru Girişi dokümanına göz atabilirsiniz.

Raporları farklı bir yerde saklayabilir miyim. Ne kadar süre ile saklamam gereklidir?

Samba veya NFS desteği vardır. Uzak sunucunuza bu raporları atabilir. 5651 nolu yasanın 6.b bendi gereği bu raporlar 2 yıl saklanmalıdır. Detaylı bilgi için Rapor Arşivi dokümanına göz atabilirsiniz.

Kimlik Doğrulamaları hangi kaynaklardan yapabilirim ?

Hotspot, Proxy, VPN gibi servislere farklı kimlik sağlayıcılar ile kimlik doğrulama politikası atanabilmektedir. Desteklenen Kaynaklar;

- Yerel Kaynaklar
- HTTP (Doğrulama)
- LDAP
- SSO : Negotiate/Kerberos - Active Directory
- RADIUS
- SMS
- Yerel Gruplar
- POP3 / IMAP
- HTTP (Api)
- TACACS+

Detaylı bilgi için Yerel Kullanıcılar dokümanına ve Hotspot HTTP API Entegrasyonu, Hotspot HTTP Doğrulama Entegrasyonu, Hotspot LDAP Entegrasyonu, Hotspot POP3 - IMAP Entegrasyonu, Hotspot RADIUS Entegrasyonu, Hotspot SMS Entegrasyonu, Hotspot Yerel Kullanıcı yapılandırma örneklerine göz atabilirsiniz.

Hotspotta ne gibi destekler vardır ?

Süre bazlı kota desteği, Trafik bazlı kota desteği, Kota limitlerinin hesap ile ilişkili olarak takibi, Kişi başı oturum açma limiti, Oturum bilgi penceresi kapanmasına rağmen trafiğe devam etme desteği, Yazılıma entegre Hotspot modülü, kurum içinde bulunan personel, öğrenci mail adresleri veya öğrenci bilgi sistemleri ile beraber çalışabilir yapıdadır, Hotspot servisine dahil olacak istemci/networkler ve hariç tutulacak istemci ve networkler olarak tanımlanabilir. Yazılım, MERNİS sunucularından kimlik bilgilerini doğrulanabilmektedir. İstendiği takdirde SMS ile kimlik bilgisi doğrulama işlemi yapabilmektedir. Servisin LDAP, Active Directory, RADIUS, POP3, IMAP, POP3 SSL, IMAP SSL, JSON Web Servis, XML Web Servis entegrasyonları bulunmaktadır. Detaylı bilgi için Hotspot Ayarları dokümanına göz atabilirsiniz.

Uygulama Güvenliği performansı ve tanıdığı uygulama ne kadardır ?

RSS duyarlı Multithreaded Uygulama Tanıma motoru sayesinde yüksek performans sağlar. Geniş AppID veritabanı ile 4500'ün üzerinde uygulamayı tespit eder. Sistem internet üzerinden uygulama imzalarını otomatik güncelleyebilmektedir. Sistem Layer 7 Derin paket inceleme yapabilmekte, uygulama imzalarını tespit edip engelleyebilmektedir. Detaylı bilgi için Uygulama Güvenliği ve IPS Ayarları dokümanına göz atabilirsiniz.

Saldırı Tespit ve Önleme (IPS) de hangi tür saldırıları önler ?

Antikor NGFW, Multi-threaded Analiz Motoru ile hızlı ve güçlü olarak saldırı tespiti yapar. Kural tabanlı tanımlama yaparak, her istemci veya ağa farklı uygulama filtrelerini çalıştırabilirsiniz:

- İmza Tabanlı Saldırı Tespit ve Önleme

- ARP Zehirlemesi Saldırısı Tespiti ve Önleme
- SYN Flood Saldırısı Tespiti ve Önleme
- UDP Flood Saldırısı Tespiti ve Önleme
- DoS Saldırısı Tespiti ve Önleme

Detaylı bilgi için Saldırı Tespit ve Önleme dokümanına göz atabilirsiniz.

Antikorda kullanılan NAT çeşitleri nelerdir ?

Dinamik NAT, Statik NAT, Hedefe Göre NAT, Port Yönlendirme'dir. Detaylı bilgi içinDinamik NAT, Statik NAT, Hedefe Göre NAT ve Port Yönlendirme dokümanlarına göz atabilirsiniz.

DNS Filtreleme seçenekleri nelerdir, nasıl yapabilirim ?

DNS ile engelleme işlemi yapılmakta olup; Alan Adları, Adres Bazlı, Aktif Saat Dilimi, Kategori Bazlı Yapılandırma yazılabilmektedir. İstemci gruplarına göre farklı politikalar oluşturulabilmektedir. Detaylı bilgi için DNS Filtreleme dokümanına ve DNS Filtreleme Adres Bazlı Yapılandırma, DNS Filtreleme Aktif Saat Dilimi Yapılandırması, DNS Filtreleme Güvenli Arama Yapılandırması, DNS Filtreleme Kategori Bazlı Yapılandırma örneklerine göz atabilirsiniz.

Web sitesi bazlı belirlediğim siteleri Antikorun ön belleğine alabilir miyim ?

Önbelleğe Alınacak Siteler bölümünde Kullanıcıların çok sık ziyaret ettiği siteler ve update yapan programların isimleri buraya yazılır. Örnek olarak Windows ve antivirüslerin adreslerin güncelleme adresleri yazılabilir. Bu sayede ilk indiren kişiden sonra diğerleri otomatik güncellemelerini bu servisten alır. Detaylı bilgi için Önbelleğe Alınacak Siteler dokümanına göz atabilirsiniz.

Bazı sitelerin hızını nasıl limitlerim ?

Hızı Limitlenecek Siteler bölümüne girilen sitelerin hızını istemci başına, o VLAN'daki(networkteki) kullanıcıların toplamını Network başına, bütün VLAN'ların toplamını da toplam kategorisine sınırlar. Özellikle rapidshare, megaupload, hotfile gibi siteler girilir. Detaylı bilgi için Hızı Limitlenecek Siteler dokümanına göz atabilirsiniz.

Web Filtreleme ve DNS Filtreleme için Kategori Yönetimi yapabilir miyim ?

Kategori Yönetiminde İsteğe göre kategori eklenebilmektedir. Antikor üzerinde de yüzden fazla ön tanımlı kategori bulunmaktadır. Bunlardan istenilen kategorilere izin verilip istenilenlere Web ve DNS Filtrelemede engelleme yapılabilir. Detaylı bilgi için Kategori Yönetimi dokümanına göz atabilirsiniz.

Antikor üzerinde Sunucularımı yerel ağdan nasıl ayırırım, Seçeneklerim nelerdir ?

Antikor üzerinde 3 farklı Sunucuları ayırma türü vardır;

1. NAT yapma, olduğu gibi Erişim → DMZ bölgesinde gerçek IP kullanılır. Yine bu IP lere belirli portlar açılıp kapatılabilir.
2. Her yönde NAT yap → DMZ bölgesinde sanal IP ler kullanılır. Hem yerel ağdan hemde dış dünyadan bu sunucuya NAT yapılarak girilir.
3. Sadece WAN'da NAT yap → Yerel ağımızdan sanal IP ile sunucuya ulaşılırken dış dünyadan NAT ile ulaşılır.

Detaylı bilgi için "Her Yönde NAT Yap" Yapılandırması, "NAT Yapma, Olduğu Gibi Erişim" Yapılandırması ve Sadece WAN dan Gerçek IP Erişimi Yapılandırması örneklerine göz atabilirsiniz.

Antikor üzerinde hangi VPN türlerini kullanabilirim ?

IPSEC VPN, L2TP/PPTP VPN, SSL VPN, Site to Site VPN türleri kullanılabilir. Detaylı bilgi içinIPSEC VPN Ayarları, L2TP/PPTP VPN Ayarları, SSL VPN Ayarları ve Site to Site VPN Ayarları dokümanlarına göz atabilirsiniz.

Antikor üzerinde Kural Tabanlı Yönlendirme yapabilir miyim ?

PBR; Protokol (IP, TCP, UDP, ICMP …), Kaynak Adres (IPv4 / IPv6), Kaynak Port, Hedef Adres (IPv4 / IPv6), Hedef Port kriterlerine göre yapılmaktadır. Detaylı bilgi için Kural Tabanlı Yönlendirme dokümanına göz atabilirsiniz.

MAC adresini dağıtan bilgisayarları nasıl karantinaya alırım ?

Antikor Karantina Durumunda, Layer 2 seviyesinde arp zehirlenmesi yapan ve kendini ağ geçidiymiş gibi gösterip, MAC adresini dağıtan bilgisayarları karantinaya alır. Bundan sonra o MAC adreslerine kullanılmayan bir IP bloğundan IP vererek ağın zehirlenmesinin önüne geçer.
Sistem yöneticisi web yönetim panelinden o MAC adresini karantinadan çıkarmadığı sürece o bilgisayar internet erişimi engellenir. Ayrıca elle de istediğimiz MAC adresini ekleyerek internete çıkmasını engelleyebiliriz. Detaylı bilgi için Karantina Durumu dokümanına göz atabilirsiniz.

Antikor üzerinde saldırganlar için tuzak portlar açabilir miyim ?

Balküpü servisinde, port taramalarını ve popüler hizmetlere bağlantıları tespit edebilen tuzaklardır. Sisteme tuzak ve çok saldırılan portlar girilir. Sistem sahte olarak bu portları açar. Bu portlara saldırı yapanları seçilen “Engelleme Süresi” kadar yasaklar. Kendi ağımızda “Gözardı Edilecekler” e kendi IP lerimizi girebilir ve hariç tutabiliriz. Detaylı bilgi için Balküpü Ayarları dokümanına göz atabilirsiniz.

Antikor sunucumu değiştireceğim, Üzerindeki kullanıcı ve ayarları nasıl aktaracağım ?

Antikor’daki bütün ayarlar kendi bilgisayarımıza alınıp, geri yükle ile istenildiği zaman yedekten geri dönülebilir veya bu ayarlar başka Antikora yüklenebilir. İndir butonuna basılarak yedek bilgisayarımıza kaydedilir. Antikor ayar yedekleri FTP, SAMBA, SCP, NFS, SFTP kullanarak yıllık, aylık, haftalık ve günlük olmak üzere otomatik harici bir sunucuya atabilmektedir. Detaylı bilgi için Yedekle / Geri Yükle dokümanına göz atabilirsiniz.

Antikor üzerindeki önemli olaylardan nasıl haberdar olabilirim ?

Antikor üzerindeki önemli durumlar Bildirim Sistemine tanımlanır. Bu bildirimlerin gideceği grup ve kullanıcılar da tanımlanır. Hangi metodla ulaştırılacağı da tanımlanır. Örneğin CPU, Ram, Disk kullanımının belirtilen değeri aşması veya ethernetlerin kapatılıp açılması gibi. Detaylı bilgi için Bildirim Geçmişi dokümanına göz atabilirsiniz.