YÖNLENDİRME GÜVENLİĞİ İÇİN KARŞILIKLI ANLAŞILAN İLKELER MANRS

Çeviren ve Derleyen: Gökhan ERYOL
Haziran 2020

MANRS Eğitim Belgelerinden ISOC TR için hazırlanmıştır.

Eğitmen: Max Larson ISOC TR Bölüm Koordinatörü: Serkan Orcan

GİRİŞ

Bu belge, 13 Nisan 2020 tarihinde ISOC (Internet Society) tarafından verilen ***"Yönlendirme Güvenliği için Karşılıklı Anlaşılan İlkeler – Mutually Agreed Norms of Routing Security – MANRS"*** eğitimi kapsamında, tamamlama konusu olarak eğitim belgelerinin Türkçe'ye çevrilmesi kapsamında hazırlanmıştır. Eğitimin amacı, bölgesel bilgiyi artırmak ve farkındalık oluşturarak toplam küresel yönlendirme güvenliğini artırmaktır.

Eğitim belgeleri https://www.manrs.org/resources/tutorials/ adresinde yer almaktadır.

Belge, yerel ve küresel ağ yönetimi yapmış, dinamik protokoller ve özellikle BGP konularında iyi derecede bilgi sahibi kişilere yönelik hazırlanmıştır.

1. TEMELLER

KÜRESEL YÖNLENDİRME

İnternet üzerinde, yaklaşık 60.000 adet otonom sistem yer almaktadır. Her otonom sistem, kendisine ait bir ASN (Autonomus System Number) numarasına sahiptir. Yönlendiriciler, sınır yönlendirme protokolü BGP (Border Gateway Protokol) kullanarak, ağların erişilebilirlik bilgilerini birbirleri ile paylaşıp yönlendirme tablolarını oluştururlar. Küresel İnternet üzerinde erişilebilir olmanın yolu, bu bilgi değiş tokuşuna dahil olmaktan geçer.

YÖNLENDİRME KESİNTİLERİ

Yönlendiricilerin paylaştığı yönlendirme tabloları, çeşitli sebeplerle kesintiye uğramaktadır. Sadece 2017 yılında, 14.000 yönlendirme kesintisi ve/veya atak yaşanmıştır. Bu durumlar, veri hırsızlığına, maddi kayba, itibar zedelenmesine ve benzeri sonuçlara neden olmuştur. Yaşanan kesintilerin yaklaşık %40 kadarı saldırı nedeniyle olmaktadır ve bu kesintilerin her biri ortalama 19 saat sürmektedir. Kesintiler küresel ölçekte yaşanmakta, bir operatörün yaşadığı yönlendirme sorunu, domino etkisi ile yönlendirici komşuluğundaki operatörlere yansımaktadır.

Konuya örnek olabilecek bazı kesintiler,

- 24 Şubat 2008 Pakistan Telecom (AS17557) tarafından yetkisiz bir şekilde 208.65.153.0/24 aralığını anons etmesi, ve üst servis sağlayıcısının bu anonsu küresel İnternet'e anons etmesi ile oluşan YouTube trafik kesintisi:
  https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

- 1 Nisan 2020 tarihinde, Rostelecom (AS12389) tarafından, Amazon, Akamai ve Level3, Alibaba, Digital Ocean, Linode servis sağlayıcılarına ait bazı IP aralıklarını anons etmesi vakası:
  https://www.manrs.org/2020/04/not-just-another-bgp-hijack/
  https://blog.qrator.net/en/how-you-deal-route-leaks_69/

YÖNLENDİRME TEHDİTLERİ

BGP KAÇIRILMASI (BGP HİJACKİNG)

Kaçırılma (hijacking), uçak kaçırma örneğinde olduğu gibi bir saldırgan tarafından yönlendirici tablolarının saldırgan menfaatine değiştirilmesi şeklinde olabileceği gibi, ağ yöneticileri tarafından yanlışlıkla da gerçekleşebilir. BGP kaçıran yönlendirici, kendisine ait olmayan başka bir ağı kendi anonsları arasında gibi göstermesi ile oluşur. Bu yanlış bilgi komşu ağlar tarafından kabul edilir ve küresel İnternet'e yayılarak İnternet haritasını bozar.

Ağ üzerinde paketlerin yanlış yere yönlendirilmesi, servis dışı bırakma saldırısı – DoS veya trafiğin saldırganlarca yakalanması, durdurulması gibi sonuçlar doğurur. Operatörler tarafından güçlü rota filtreleri yazılarak engellenebilir.

Rota Sızıntısı (Route Leak)

Çoklu komşuluğu olan ağ operatörlerinin, komşuluklar ile yaptığı çeşitli anlaşmalar vardır ve bu koşullar gereği öğrenilen rotaları sadece belirli gruplara anons etmesi kararlaştırılmış olabilir. Rota sızıntısı, diğer komşuluklara anons edilmemesi gereken bazı iç veya özel komşuluk rotalarının anons edilmesi ve dolayısıyla amaçlanan kapsamının ötesine yayılması durumudur. Bu durum genellikle yanlış yapılandırma sonucu oluşur.

Bu durum, sızan rotaya olan trafiğin kesilmesine neden olabileceği gibi, yetkisiz kişilerce trafiğin izlenmesine neden olabilir. Operatörler tarafından rota filtreleri yazılarak engellenebilir.

IP Adres Sahteciliği (Spoofing)

IP adresi sahteciliği veya IP sahtekarlığı, gönderenin kimliğini gizlemek veya başka bir bilgi işlem sisteminin kimliğine bürünmek amacıyla, IP paketlerinde kaynak IP adresi alanına müdahale ederek değiştirilmesi durumudur. Yansılanan dağıtık servis dışı bırakma (reflection DDoS) saldırılarında kullanılır. Kaynak adres doğrulama yöntemi ile engellenebilir.

MANRS - Yönlendirme Güvenliği İçin Karşılıklı Anlaşılan İlkeler

MANRS, Yönlendirme Güvenliği için Karşılıklı Anlaşılan İlkeler, Internet Society tarafından desteklenen ve yaygın yönlendirici tehditlerini azaltmayı sağlayan küresel bir girişimdir. Bu girişime göre servis sağlayıcılar başta olmak üzere tüm ağ operatörleri, İnternet'in yönlendirme altyapısının küresel güvenilirliğini ve güvenliğini sağlama sorumluluğunu taşımaktadır.

MANRS, güvenlik odaklı ağ operatörleri tarafından oluşturulmuş ve belirli ilkeleri paylaşan bir topluluktur. MANRS:

- Yönlendirme güvenliğine önem verir.
- Yönlendirme güvenliği için kaynak ayırmaya hazırdır.
- Topluluk tarafından sorumlu tutulmaya hazırdır.

Internet Society her ağ operatörüne güvenlik duruşunu güçlendirmek ve yönlendirici güvenliği olaylarının sayısını ve etkisini azaltmak için MANRS topluluğuna katılmasını önermektedir.

Servis Sağlayıcılar MANRS'a katılarak aşağıdaki amaçlara ulaşırlar:

- Rekabetçi değer katmak ve düz, fiyat odaklı bir pazarda farklılaşmak;
- Müşterilerine güvenlik yetkinliklerini ve yaklaşımlarını gösterebilmek;
- Sade bir bağlantı sağlayıcıdan ziyade, güvenlik partneri de olduklarını göstermek;
- Küresel ağ sorunlarını çözmeye yardım etmek;
- Güvenli hizmetlere daha çok yatırım yapan şirketlere ulaşmak.

Kurumların, servis sağlayıcılarının MANRS'a dahil olmasını isteme sebepleri:

- Kurumsal güvenlik duruşlarını sergilemek için;
- Ağlarını etkileyen güvenlik sorunlarını tespit edip çözebilmek için;
- Güvenlik temelli katma değerli servisler sunabilmek için.

İnternet değişim noktaları (Internet Exchange Points- IXPs) ortak amaçlar doğrultusunda bir araya gelen ve bu sayede daha esnek ve güvenli İnternet altyapısı sunabilen ağ operatörlerini barındırır. CDN ler (İçerik Dağıtım Ağları) ve bulut sağlayıcılar da onlarca diğer ağlara dahil olmakta ve trafik aktarmakta ve dolayısı ile İnternet altyapısının önemli bir parçası halindedirler. MANRS'a katılım sağlamaları halinde güvenli komşuluklar kurarak MANRS ilkeleri temelinde birleşebilir, yönlendirici güvenliği ve temiz yönlendirme tabloları sağlanması konularında müşterilerine ve topluluğa olumlu izlenim bırakabilirler.

MANRS TEMEL PRENSİPLERİ:

- Biz (İSS / ağ operatörleri / CDN ve Bulut Sağlayıcıları), küresel yönlendirme sisteminin birbirine bağlı doğasını ve güvenli ve esnek bir İnternet'e katkıda bulunmak konusundaki rolümüzü kabul ediyoruz.
- Yönlendirme güvenliği ve esnekliği ile ilgili en iyi uygulamaları ağ yönetim süreçlerimize Eylemler doğrultusunda entegre edeceğiz.
- Eylemlere uygun olarak akranlar (peer) ve diğer İSS'lerle işbirliği ve koordinasyon yoluyla yönlendirme olaylarını önlemeye, tespit etmeye ve azaltmaya kararlıyız.
- Müşterilerimizi ve meslektaşlarımızı bu İlkeleri ve Eylemleri benimsemeye teşvik ediyoruz.

MANRS, ağ operatörlerinin uygulaması gereken dört temel aksiyon tanımlamıştır: Küresel doğrulama, filtreleme, sahtecilik önleme, koordinasyon. Buna göre;

- Yönlendirme bilgilerinin küresel ölçekte doğrulanmasını kolaylaştırmak için, ağ operatörleri yönlendirme bilgilerini diğer tarafların doğrulayabilmesi için yayınlamalıdır.
- Yanlış yönlendirme bilgilerinin yayılmasını önlemek için, şebeke operatörleri kendi duyurularının ve müşterilerinin önek ve AS-yolu bilgilerinin komşu ağlara duyurularının doğruluğunu sağlamalıdır.
- Sahte kaynak IP adresleri ile trafiği önlemek için, ağ operatörleri tek bağlantıya sahip müşteri ağları, kendi son kullanıcıları ve altyapıları için kaynak adres doğrulamasını etkinleştirmelidir.
- Ağ operatörleri arasında küresel operasyonel iletişimi ve koordinasyonu kolaylaştırmak için, herkes tarafından erişilebilir ve güncel iletişim bilgilerini korumalıdırlar.

MANRS'a uymak için gerekli adımları uygulamak konusunda yardımcı olmak amacıyla, MANRS katılımcıları topluluğu bir Uygulama Kılavuzu geliştirdi. Bu belge, dünya çapında ağ operatörleri tarafından dağıtılan en iyi operasyonel uygulamaları göstermektedir. Belgeye https://www.manrs.org/isps/guide/ adresinden erişilinebilir.

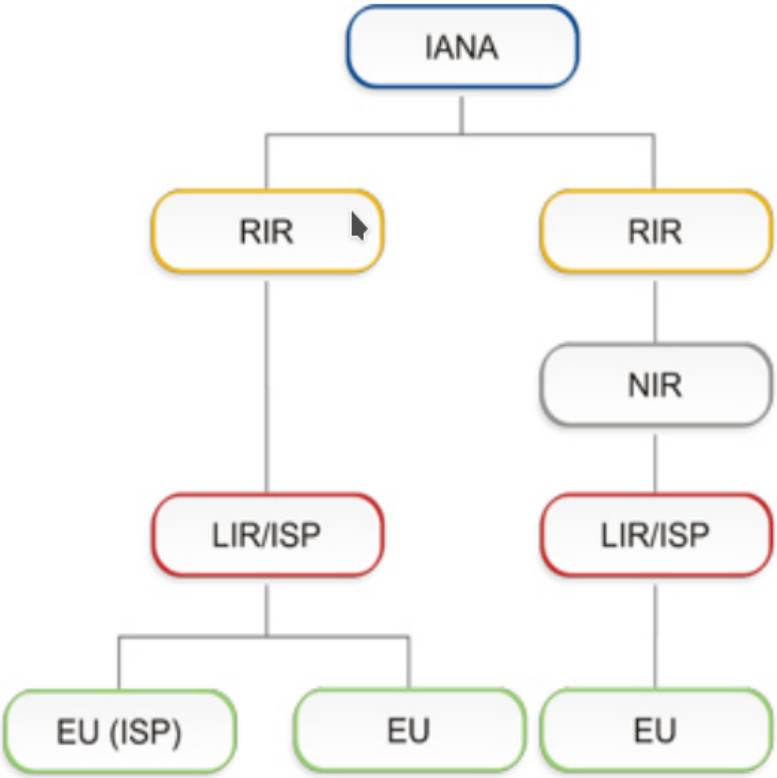
2. ARAÇLAR

Bu bölümde, MANRS katılımcılarının rota politikalarını belirlerken ve iletişim bilgilerine erişmek için kullanabilecekleri veritabanları ve bilgi depoları listelenecektir.

KAYNAK YÖNETİM HİYERARŞİSİ

İnternet numarası kaynakları, son yirmi yılda gelişen hiyerarşik bir kayıt sistemine göre küresel olarak dağıtılmaktadır. Bir kuruluşta resmileşmeden önce, IP adresleri ve AS numaraları gibi İnternet kaynaklarının tahsisi, Güney Kaliforniya Üniversitesi (USC) Bilgi Bilimleri Enstitüsü'nde (ISI) çalışmakta olan Jon Postel'in sorumluluğunda idi. Günümüzde İnternet Tahsisli İsimler ve Numaralar Kurumu ICANN (Internet Corporation for Assigned Names and Numbers) tarafından yürütülen İnternet Tahsisli Sayılar Otoritesi - IANA (Internet Assigned Numbers Authority) bu rolü üstlenmiştir.

Aşağıda, İnternet numarası kaynaklarının, IANA tarafından yönetilen havuzdan, halen beş adet olan bölgesel dağıtım yetkilisine ve oradan yerel dağıtım yetkililerine aktarılmasına dair hiyerarşi yer almaktadır.



IANA (Internet Assigned Numbers Authority)

Küresel IP adres alanının bir kısmını ve otonom sistem numaralarını Bölgesel Kayıtlara göre tahsis etmekten sorumludur. Organizasyon hakkında resmi sayfasından bilgi alınabilir: https://www.iana.org/

IR (Internet Registry)

Üyelerine veya müşterilerine IP adres alanı tahsis etmekten ve bu tahsisleri kaydetmekten sorumlu İnternet kayıt yetkilisidir. IR'ler, yukarıdaki şekilde tanımlanan hiyerarşik yapıda belirtildiği gibi ana işlevlerine ve coğrafi kapsama alanlarına göre RIR, NIR, LIR olarak sınıflandırılır.

RIR (Regional Internet Registry)

Geniş coğrafi bölgelere hizmet eden bölgesel kayıt yetkilisidir. RIR'lerin birincil rolü, İnternet kaynaklarını kendi bölgelerinde yönetmek ve tahsis etmektir. 2020 yılı itibariyle 5 RIR faaliyet göstermektedir:

REGISTRY	AREA COVERED
AFRINIC	Africa Region
APNIC	Asia/Pacific Region
ARIN	Canada, USA, and some Caribbean Islands
LACNIC	Latin America and some Caribbean Islands
RIPE NCC	Europe, the Middle East, and Central Asia

NIR (National Internet Registry)

Her ülkede uygulanmamakla beraber varsa, İnternet numara kaynaklarını ulusal ölçekte coğrafi kısıtlama ile değerlendirerek genellikle LIR olan üyelerine veya diğer bileşenlerine tahsis eder.

LIR (Local Internet Registry)

Sağladığı ağ hizmetlerinin kullanıcılarına İnternet numara kaynaklarını atayan yerel dağıtım yetkilisi IR'dir. LIR'lar genellikle İnternet Servis Sağlayıcısı - İSS dirler ve müşterileri son kullanıcı veya diğer İSS'lerdir.

Yukarıda anlatılan kayıt mekanizmalarına göre, İnternet üzerinde var olan her ağa ait IP sürüm 4 ve sürüm 6 adresleri, AS numaraları kaynakları tahsis edilmekte, tahsis edilen kaynağın sorumlu olduğu kuruma dair iletişim, adres gibi bilgiler de atanmaktadır. MANRS eylemlerini gerçekleştirebilmek için ağ operatörleri, yönettikleri ağ hakkında bilgileri çeşitli veritabanları ve bilgi depolarında yayınlarlar. Yayınlanan yerler arasında, IRRs - Internet Routing Registries, RPKI - Resource Public Key Infrastructure ve PeeringDB yer almaktadır.

IRR, Internet Routing Registry

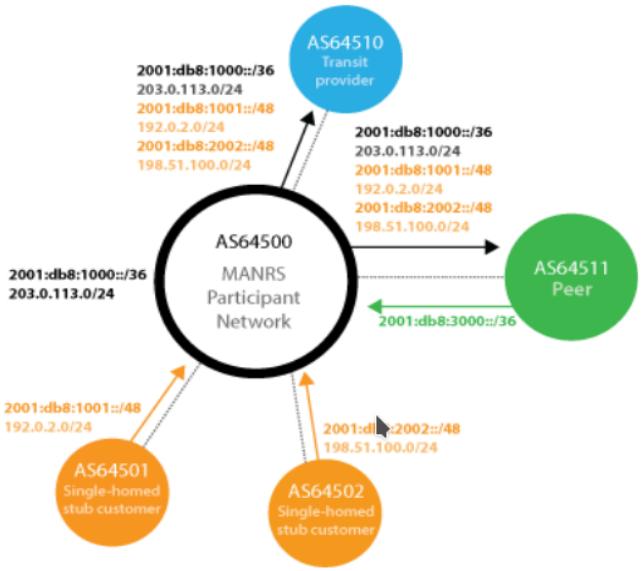
İnternet rota kayıtlarının kısaltmasıdır. IRR'ler, yönlendiricileri yapılandırmak için kullanılan rota ve diğer ilgili bilgileri belirlemek ve paylaşmak için kullanılır. MANRS katılımcısı her ağ operatörü ağı işlettiği bölgede yer alan Bölgesel İnternet Kayıt Yetkilisi - RIR (Regional Internet Registry) tarafından işletilen IRR'yi kullanarak, ağ rota politikasını ve buna bağlı olan rota anonslarını kaydederek paylaşmalıdır.

Kayıtlar RPSL (Routing Policy Specification Language) kullanarak standardize edilmiş halde paylaşılmaktadır. Küresel yönlendirme politikası veritabanlarının birliği olan IRR'nin koordinasyonunu sağlayan web sayfasına http://www.irr.net/ adresinden erişilinebilir. Sayfada güncel IRR listesi yer almaktadır. Ağ operatörü, bulunduğu bölgedeki RIR tarafından işletilen IRR var ise ağ yönlendirme politikalarını ve bağlı rota anonslarını oraya kaydetmelidir.

Bölge	Tercih Edilen IRR	Alternatif IRR
Avrupa	RIPE NCC	RADb / NTTCOM
Amerika	ARIN	RADb / NTTCOM
Afrika	AFRINIC	RADb / NTTCOM
Asya Pasifik	APNIC	RADb / NTTCOM
Latin Amerika ve Karayipler	RADb	NTTCOM

MANRS eylemlerine göre katılımcıların paylaşılması zorunlu tutulan ve RPSL ile ortak veritabanında yayınlanan ağ yönlendirme politikaları (Network Routing Policies), veriyi nesneler ile tutar. Sık kullanılan örnek olabilecek bazı nesneler: <route/>, <route6/>, <aut-num/>, <as-set/>

Aut-num nesnesi, RIR tarafından AS e atanan AS numarasına dair kayıt detaylarını içerir. Aynı zamanda ağ yönlendirme politikalarının yayınlanmasını sağlar. AS64500 örneğine bakacak olursak:




```
aut-num:        AS64500
descr:          Provider 64500
remarks:        ++ Customers ++
mp-import:      from AS64501 accept
                AS64501
mp-export:      to AS64501 announce
ANY
mp-import:      from AS64502 accept
                AS64502
mp-export:      to AS64502 announce
ANY
remarks:        ++ Peers ++
mp-import:      from AS64511 accept
                AS64511:AS-A::
mp-export:      to AS64511 announce
                64500:AS-ALL
remarks:        ++ Transit ++
mp-import:      from AS64510 accept
ANY
                except FLTR-BOGONs
mp-export:      to AS64510 announce
AS64500:AS-ALL
mnt-by:         MAINT-AS64500
created:        2012-10-27T12:14:23Z
last-modified:  2016-02-27T12:33:15Z
source:         RIPE
```

Route ve route6 nesneleri, IPv4/IPv6 adreslerine yönelik olarak AS tarafından gönderilen rota bilgisini içerir.

```
route:              2001:db8:1000::/36
descr:              Provider 64500
origin:             AS64500
mnt-by:             MAINT-AS64500
created:            2012-10-27T12:14:23Z
last-modified:      2016-02-27T12:33:15Z
source:             RIPE
```

AS-SET nesnesi, yönlendirme politikalarında kullanılmak üzere bir grup ASN i gruplamak için kullanılır. Ağ operatörünün müşterilerinin olduğu bir grup, veya ağın özel bir grubu olarak kullanılabilir. Aşağıdaki örnekte, AS64500 ün iki müşteri ağının gruplanmış hali görülmektedir.

```
as-set:             AS64500:AS-CUSTOMERS
descr:              AS64500 regional customers
members:            AS64501, AS64502
tech-c:             EXAMPLE1-AP
admin-c:            EXAMPLE2-AP
mnt-by:             MAINT-AS64500
last-modified:      2008-09-04T06:40:26Z
source:             APNIC
```

RPKI - Resource Public Key Infrastructure

IRR bilgilerinin yanısıra, ağınıza dair rota bilgilerinin RPKI depolarına kaydedilmesi önerilmektedir. Bu kayıt, ROA - Route Origin Authorization nesnesi kullanılarak yapılmaktadır. ROA nesneleri kriptografik olarak imzalanmış, AS tarafından hani IP aralıklarının gönderilebileceği bilgisini içeren nesnelerdir.

ROA nesneleri oluşturulurken (yönlendirilecek IP aralıkları belirlenirken) AS tarafından duyurulmasına izin verilen en spesifik uzunluk konusuna dikkat edilmeli, belirtilenden daha dar aralık kullanılmamalıdır. Daha geniş aralık kullanılması durumunda da, yönlendirme tablolarında dar olanın önceliği olduğu unutulmamalıdır.

PeeringDB

PeeringDB, ağların komşuluk için gerekli eşleşme (peering) bilgilerini ve diğer ilgili bilgileri birbirleriyle paylaşmaları için açık bir kaynaktır. Her ağ kendi kaydını tutmaktan sorumlu olup, PeeringDB kaydı ile ağ bilgileri tek bir yerde birleştirilir ve diğer ağlar hakkında bilgi aranması mümkün olur.

PeeringDB yı kullanmak için siteye kayıt olunduktan sonra hesabın kuruluşa veya ASN e bağlanması talep edilir. Onay sonrası tüm alanların güncellemesi yapılabilir. Aşağıdaki örnekte Türk Telekom kuruluşuna ait PeeringDB kaydı görülmektedir.

PeeringDB

Search here for a network, IX, or facility.

Advanced Search

Register or Login

Turk Telekom

Organization	Turk Telekom
Also Known As	
Company Website	http://www.turktelekom.com.tr
Primary ASN	9121
IRR as-set/route-set	AS-TTNET
Route Server URL	
Looking Glass URL	http://lg.turktelekom.com.tr/lg/
Network Type	NSP
IPv4 Prefixes	18000
IPv6 Prefixes	800
Traffic Levels	Not Disclosed
Traffic Ratios	Mostly Inbound
Geographic Scope	Europe
Protocols Supported	✓ Unicast IPv4 ○ Multicast ✓ IPv6 ○ Never via route servers
Last Updated	2020-03-31T13:24:38Z
Notes	

Peering Policy Information

Peering Policy	
General Policy	Selective
Multiple Locations	Preferred
Ratio Requirement	Yes
Contract Requirement	Not Required

Contact Information

Some of this network's contacts are hidden because they are only visible to authenticated users and you are currently not logged in.

Public Peering Exchange Points

Filter

Exchange ASN	IPv4 IPv6	Speed RS Peer
AMS-IX 9121	80.249.208.241 2001:7f8:1::a500:9121:1	200G ○
DE-CIX Frankfurt 9121	80.81.192.82 2001:7f8::23a1:0:1	200G ○

Private Peering Facilities

Filter

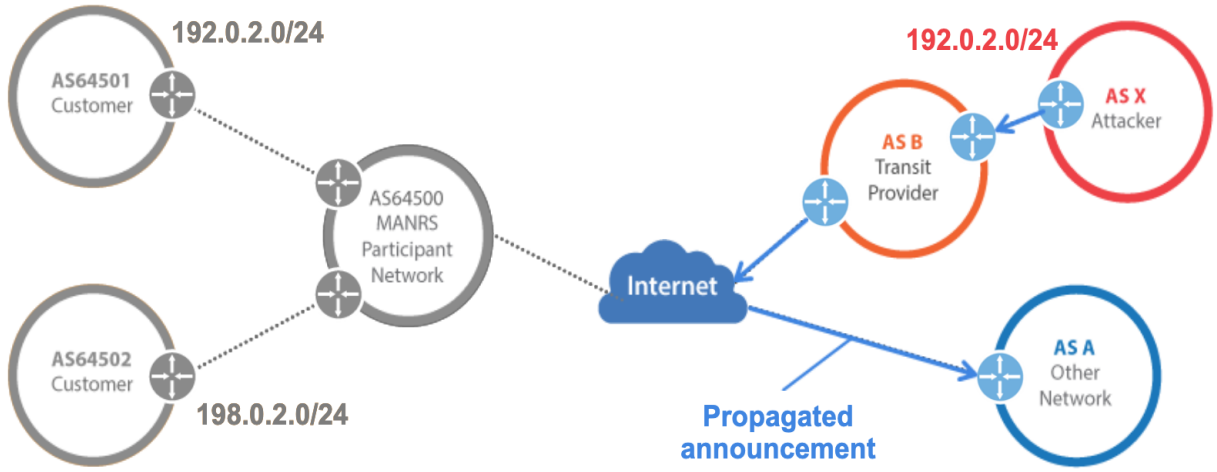
Facility ASN	Country City
Digital Realty AMS (Science Park) 9121	Netherlands Amsterdam
Equinix FR7 - Frankfurt, Gutleutstrasse 9121	Germany Frankfurt
IRIDEOS Avalon Campus 9121	Italy Milan
Interxion Marseille (MRS1, MRS2) - previously called SFR Netcentre 9121	France Marseille
Interxion Vienna (VIE1, VIE2) 9121	Austria Vienna
NXDATA-1 Bucharest Romania (BU1) 9121	Romania Bucharest
TELEPOINT Sofia Centre 9121	Bulgaria Sofia

3. KÜRESEL DOĞRULAMA

Bu bölümde bir Ağ Yönlendirme Politikası oluşturarak ağdan yapılan rota duyurularını, diğer ağ operatörlerinin nasıl doğrulayabileceği anlatılmaktadır. Ağ Yönlendirme Politikasının ne olduğu, kuruluşun Ağ Yönlendirme Politikasını nasıl oluşturacağı ve ağdan gelen bildirimlerin doğrulanabilmesi için nasıl herkes tarafından erişilebilir hale getirilebileceği anlatılmaktadır.

MANRS katılımcıları, rota duyurularının doğrulanabilmesi için aşağıdaki eylemleri gerçekleştirmelidir:

- Komşu ağlara doğru duyurular gönderilmeli
- Dış ağlara duyurulan Ağ Yönlendirme Politikası, ASN'ler, önekler bilgilerini herkes tarafından erişilebilecek şekilde yayınlamalı.



Yukarıdaki örnekte, AS64501 AS numarasına sahip kuruluşa ait olan 192.0.2.0/24 önekli ağ, İnternete başka bir noktadan bağlı X AS numarasına sahip saldırgan tarafından kendi arkasında gibi duyurulmaktadır. Bu duyuru İnternet'e yayılarak yakın komşuluktaki AS A ve AS B tarafından kabul edilmekte, yakın komşulukta olması nedeniyle A ve B AS numaralı kuruluşlar tarafından bu rota tercih edilerek 192.0.2.0/24 ağına giden trafik AS X tarafından kaçırılmaktadır (BGP Hijacking).

Ancak AS B kuruluşu doğrulama yapıyor olursa, IRR ye soracağı

"192.0.2.0/24 öneki kime aittir"

sorusuna cevaben, AS 64501 tarafından önceden oluşturularak IRR ye yüklenmiş bilgiye ulaşarak

"192.0.2.0/24 IPv4 öneki AS 64501 e aittir"

cevabını alacak ve trafiği AS 64501 e yönlendirecektir.

Bu doğrulama sürecine Kaynak Doğrulama - Origin Validation adı verilir.

Örnekte yer alan AS 64500 kuruluşu MANRS Katılımcısı olduğu için bu doğrulamayı yaptığına güvenilmektedir.

Kaynak Doğrulama için MANRS katılımcılarının sağlaması gerekenler:

1. Ağlarına dair **aut-num** nesnesini ve dış ağlarca beklenmesi gereken duyurularına dair **route** nesnesini oluşturarak IRR ye kaydetmelidir.
2. Kendisine bağlı ağlar için **as-set** nesnesini oluşturmalıdır.
3. Bağlı ağların beklediği duyurular için **route** nesnesi oluşturup kayıt ettiğini kontrol etmelidir.
4. Kendi ve arkasındaki ağlara dair beklenen duyurular için **ROA** nesnelerinin oluşturulup kayıt edilmesini sağlamalıdır.

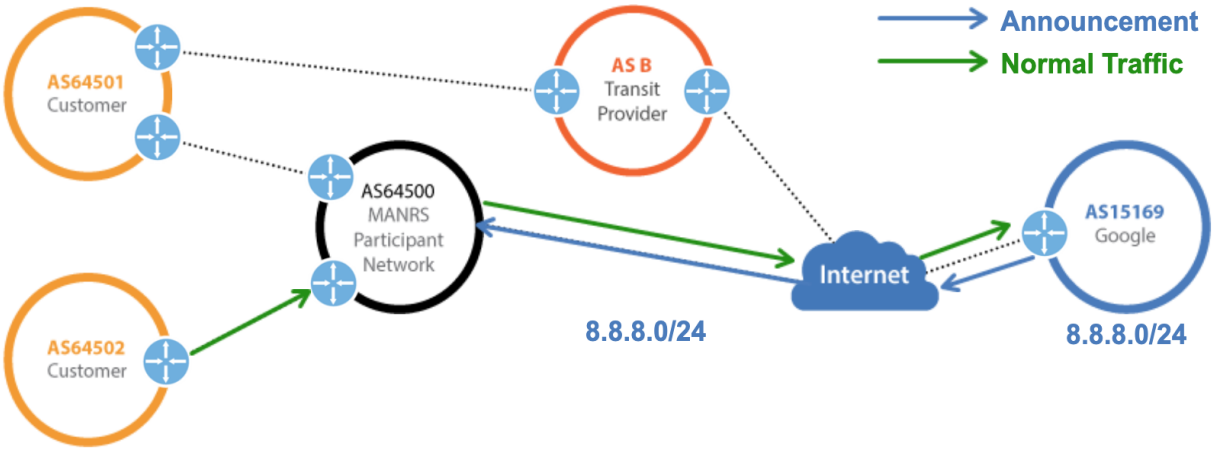
Bu işlemlerin nasıl yapılabileceğine dair genel bilgi 2. bölümde verilmiştir. Ek olarak, RIPE NCC tarafından ROA nesnesi oluşturmaya yönelik hazırlanan belgeye

https://www.ripe.net/manage-ips-and-asns/resource-management/certification/resource-certification-roa-management adresinden erişilebilinir.

4. FİLTRELEME

MANRS katılımcıları, hatalı rota bilgilerinin yayılmasını önlemek için önek filtreleme uygulamak zorundadır. Filtreleme çalışmaları kapsamında;

- Önek filtreleme ile komşu AS lerden gelecek duyurulara izin verilebilir veya engellenebilir.
- Ağ operatörleri özellikle bağlı ağlardan (müşterilerinden) gelecek rota duyurularına önek filtreleme uygulamalı, dolayısıyla dış dünyaya yaptığı kendi duyurularını güvene almalıdır.
- AS-path filtreleri kullanarak hangi AS lerin müşteri ağına yönlenmesi gerektiği belirlenebilir.



Yukarıdaki örnekte, AS64501 kuruluşunun iki ayrı bağlantısı olduğu görülmektedir. Kuruluş, İnternet ile olan bağlantısını AS64500 üzerinden yapmak, ayrıca AS B kuruluşu ile bir komşuluk kurarak kendi ağları arasındaki trafiği bu bağlantıdan geçirmek istemektedir. Ancak AS B Kuruluşunun ayrı bir İnternet bağlantısı bulunmakta olup, önek filtreleme kullanmayarak AS 64501 ile arasındaki bağlantıyı yanlışlıkla bu İnternet bağlantısından anons eder ise, İnternet üzerindeki ağlar yönlendirme tablolarında iki farklı rota görecek ve yakın olanı tercih edeceklerdir. Bu duruma rota sızıntısı/kaçağı (route leak) denilmektedir.

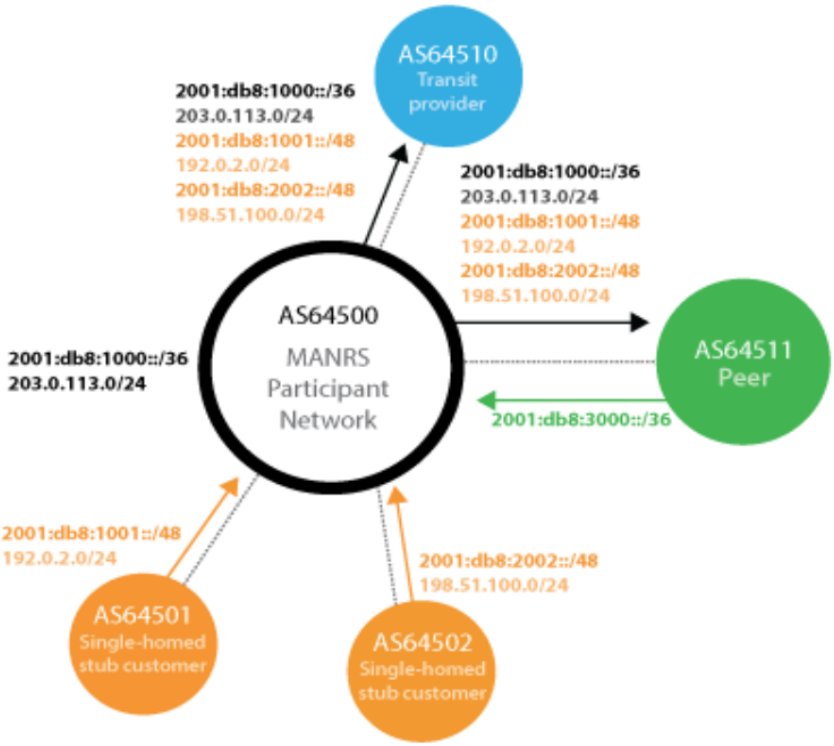
Önek filtreleme yapılabilmesi için öncelikle bağlı ağlardan hangi duyuruların beklendiği konusu netleştirilmelidir. Önek bilgileri bağlı ağlardan doğrudan talep edilebilir, ancak bu yöntem verimsiz ve çağdışı kalmıştır. Önerilen güncel ve verimli uygulama, bağlı ağların kendi bilgilerini IRR ve RPKI depolarına kaydetmelerini sağlamak ve bilgiyi bu depolardan temin etmek şeklindedir.

Filtreler oluşturulmadan önce, müşteri tarafından sağlanan bilgilerin kimlik ve kaynak doğruluğu yapılması önemlidir. Bilgiyi gönderen bağlı ağ başka bir kuruluşun adres bilgilerini girerse, ek doğrulama yapılmadan filtre oluşturulması yanlış rota duyurusu yapılmasına neden olacaktır. Bu sebeple, kuruluşa atanmış Internet numara kaynaklarını (Ip adresleri, AS numaraları, anons edilecek adres uzayı gibi) kontrol etmek önerilmektedir.

Kontrol, bölgenin bağlı olduğu RIR a ait whois veritabanına sorularak yapılabilir. https://stat.ripe.net gibi web servisleri bölgeyi ve ait olduğu RIR'ı belirlemek için kullanılabilir.

MANRS katılımcıları, bağlı ağlarının rota nesnelerini IRR kaydetmesini sağlamalı ve RPKI ile ROA kaydı oluşturulmasını sağlamalıdır. MANRS katılımcıları IRR kullanarak:

1. Kuruluş kendi ve bağlı müşteri ağlarına dair belirlenmiş spesifik önekleri, üst bağlantı sağlayıcılarına ve özel komşuluklarına doğru filtrelemelidir.
2. Kuruluş bağlı müşteri ağlarından gelen bilgiyi filtrelemelidir.
3. Özel komşu ağlar ile olan bağlantılarına, önek giriş filtresi uygulayabilir. Bu filtre en az iç ağlarda kalması gereken bogon adreslerin girişini engelleyecek şekilde yapılabilir.



Yukarıda verilen örnek topolojiye göre AS 64500 kuruluşu, kendisine bağlı iki müşteri ağı olan (AS 64501 ve AS 64502), küresel İnternete AS 64510 üzerinden ulaşan ve AS 64511 ile özel komşuluğu bulunan, MANRS katılımcısı bir ağdır. Bu senaryoya ve yukarıda anlatılanlara göre AS 64500 kuruluşunun ağ operatörü aşağıdaki adımları izler.

1. *Kendi bağlı ağlarının kayıtları olmalı, doğruluğu kontrol edilmelidir.*

AS 64501 Route nesnesi

```
route:192.0.2.0/24
descr:Cust 64501
origin: AS64501
mnt-by: MAINT-AS64501
created:2015-09-27T12:14:23Z
last-modified: 2015-09-27T12:14:23Z
source: RIPE

route6: 2001:db8:1001::/48
descr:Cust 64501
origin: AS64501
mnt-by: MAINT-AS64501
created:2015-09-27T12:14:23Z
last-modified: 2015-09-27T12:14:23Z
source: RIPE
```

AS 64502 Route nesnesi

```
route:198.51.100.0/24
descr:Cust 64502
origin: AS64502
mnt-by: MAINT-AS64502
created:2015-09-27T12:14:23Z
last-modified: 2015-09-27T12:14:23Z
source: RIPE

route6: 2001:db8:2002::/48
descr:Cust 64502
origin: AS64502
mnt-by: MAINT-AS64502
created:2015-09-27T12:14:23Z
last-modified: 2015-09-27T12:14:23Z
source: RIPE
```

2. *Kuruluş kendi **route** nesnesini oluşturarak kaydetmeli, bağlı ağları **as-set** nesnesi ile tanımlamalı ve **aut-num** nesnesi ile rota politikasını yayınlamalıdır.*

route nesnesi

```
route:203.0.113.0/24
descr:Provider 64500
origin: AS64500
mnt-by: MAINT-AS64500
created:2012-10-27T12:14:23Z
last-modified: 2016-02-
27T12:33:15Z
source: RIPE
```

route6 nesnesi

```
route6: 2001:db8:1000::/36
descr:Provider 64500
origin: AS64500
mnt-by: MAINT-AS64500
created:2012-10-27T12:14:23Z
```

as-set nesneleri

```
as-set: AS64500:AS-CUSTOMERS
members:AS64501
members:AS64502
mnt-by: MAINT-AS64500
created:2012-10-27T12:14:23Z
last-modified: 2016-02-
27T12:33:15Z
source: RIPE
as-set: AS64500:AS-ALL
members:AS64500
members:AS64500:AS-CUSTOMERS
mnt-by: MAINT-AS64500
created:2012-10-27T12:14:23Z
last-modified: 2016-02-
27T12:33:15Z
source: RIPE
```

aut-num nesnesi

```
aut-num:AS64500
descr:Provider 64500
mp-import: from AS64500:AS-
CUSTOMERS
accept PeerAS AND <^PeerAS+$>
mp-export: to AS64500:AS-
CUSTOMERS announce ANY
mp-import: from AS64510 accept
ANY except FLTR-BOGONS

mp-export: to AS64510 announce
AS64500:AS-ALL
mnt-by: MAINT-AS64500
created:2012-10-27T12:14:23Z
last-modified: 2016-02-
27T12:33:15Z
```

3. *Bu bilgiler ışığında giriş ve çıkış yönlerinde filtrelerini oluşturarak uygulamalıdır.*

Filtreler oluşturulurken IRR sorgulayarak elde ettiği **aut-num** nesnesini ayrıştırarak giriş çıkış filtreleri oluşturabilen araçlar kullanılabilir. Bu araçlardan kullanılması önerilen bazıları:

- IRRTOOLSET: Karmaşık da olsa güçlü bir araçtır. Ağ operatörlerine yönlendirici yapılandırması, yönlendirici politika analizi gibi otomatize edilebilen özellikler sunar. Detaylı bilgi ve kurulum için: https://github.com/irrtoolset/irrtoolset
- BGPQ3: Basit bir komut satırı aracıdır. IRR veritabanına bağlanır ve topladığı bilgiler ile IPv4 ve IPv6 önek listeleri oluşturur. Kurulum sonrasında nasıl çalıştığına dair örnek aşağıda verilmiştir. Girilen komutta **-4** parametresi IPv4 öneki listesi istenildiğini ve -l parametresi listenin adını belirtir.

```
$ bgpq3 -4 -l AS64500-v4 AS64500:AS-ALL
no ip prefix-list AS64500-v4
ip prefix-list AS64500-v4 permit 203.0.113.0/24
ip prefix-list AS64500-v4 permit 192.0.2.0/24
ip prefix-list AS64500-v4 permit 198.51.100.0/24
```

- IRRPT: PHP tabanlı bir yazılımdır. BGPQ3 ile benzer şekilde komut satırından çalışan bir önek listeleme aracı olmakla beraber, yapılandırma dosyalarını kullanarak seçenekleri ve ASN leri çıkarır, öneklerdeki değişimleri takip eder ve bu değişiklikler için yöneticilere alarm oluşturabilir. Ürettiği çıktı, yönlendiricinizin marka modeline göre doğrudan gönderebileceğiniz yapılandırma biçimindedir. Kurulum sonrası kullanım örneği:

```
$ ./bin/irrpt_pfxgen 64500
conf t
no ip prefix-list CUSTOMER:64500
no ip prefix-list CUSTOMERv6:64500
ip prefix-list CUSTOMER:64500 permit 203.0.113.0/24
ip prefix-list CUSTOMER:64500 permit 192.0.2.0/24
ip prefix-list CUSTOMER:64500 permit 198.51.100.0/24
ipv6 prefix-list CUSTOMERv6:64500 permit 2001:db8:1000::/36 le 48
ipv6 prefix-list CUSTOMERv6:64500 permit 2001:db8:1001::/48 le 48
ipv6 prefix-list CUSTOMERv6:64500 permit 2001:db8:2002::/48 le 48
end
write mem
```

Önek filtresi hazırlandıktan sonra dikkatle kontrol edilmeli, sonra uygulanmalıdır. Basit bir hata trafikte yanlış yönlendirmelere sebep olabilir. Bu sebeple filtreler uygulanmadan önce sıkı kontrol edilmelidir. Kontrol edilirken aşağıdaki adımlar takip edilebilir:

1. Yazım kontrolü: Yazım hatalarına karşı filtre gözden geçirilmeli, adres aralıkları kontrol edilmelidir
2. Delta kontrolü: Genel bir filtre uygulama kuralıdır. Uygulanacak filtre toplamın %n kadarını etkiliyor ise, o filtre uygulanmamalıdır. “n” üzerinde ortak fikre varılarak belirlenmiş olmalıdır (Örn %20). Ayrıca hiçbir filtre bir uzman tarafından gözden geçirilmeden uygulanmamalıdır.
3. Beacon Önekler: Özel veya önemli öneklerin izin verilmiş olduğundan ve bogon öneklerin kesildiğinden emin olunmalıdır.

Rota duyurularını RPKI ile doğrulatma konusu, IRR ile yapıldığı gibidir. Ağ operatörü ROA nesnelerini oluşturur ve filtre oluşturulması, rota doğrulaması gibi işlemlerde kullanılmak üzere kriptografik olarak

imzalayarak depolara kaydeder. AS tarafından kullanılan adres aralığını belirten RC (Resource Certificate - Kaynak Sertifika), RIR tarafından yayınlanan güven zincirini kullanılarak imzalanır.

RIPE NCC RPKI Validator yazılımı, kullanıcı dostu web arayüzü olan ve topladığı verinin sorgulanmasını sağlayan, Java ile yazılmış bri yazılımdır. RIPE NCC web sayfasından indirilerek kurulabilir. Çalıştırıldıktan sonra, 8080 portunda doğrulama yazılımına erişim sağlayan bir web servis çalıştırır. Bu servis aracılığı ile BGP yönlendirme tablosundaki ROA lar kontrol edilebilir, ROA lar route/route6 nesneleri olarak dışa aktarılabilir. Yazılım aynı zamanda 8282 portunda RPKI-to-Router servisi çalıştırır.

Ubuntu ve Debian işletim sistemlerinde RPKI yardımcı aracı kullanmanın bir diğer yolu, apt depolarında yer alan RPKI Relying Party (Validator) yazılımını kullanmaktır. “rpki-rp” paketinin ve tüm bağımlı paketlerin kurulması ile hazır hale gelir. Yerelde tuttuğu bilgiyi saatlik güncellemek için cron görevini de kuran bu yazılıma kurulduğu sunucunun üstünde http://<hostname>/rcynic/ linki ile ulaşılabilinir.

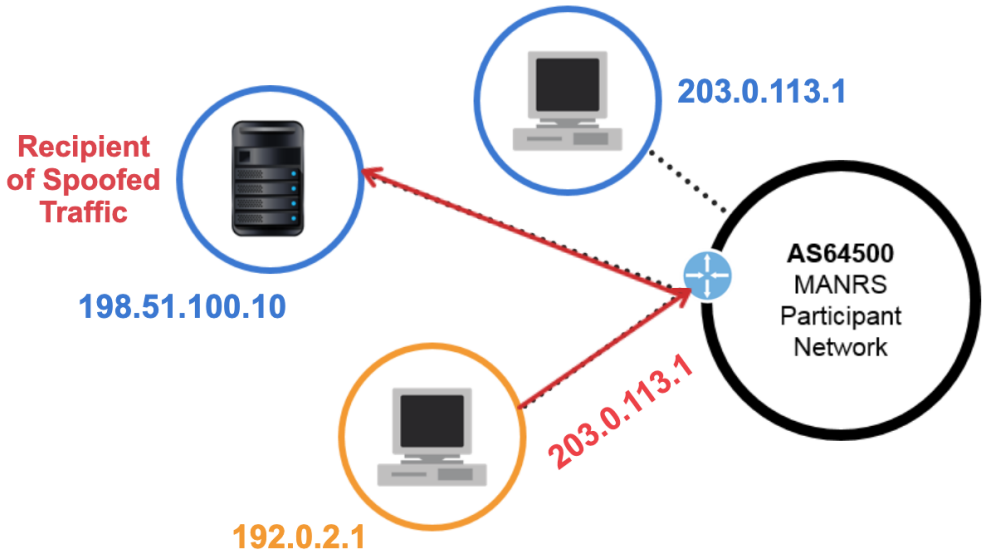
5. SAHTECİLİK ÖNLEME

Bu bölümde, ağ operatörlerinin sahtecilik önleme (anti spoofing) için neler yapabileceği anlatılmaktadır. Sahteciliği önlemek için adımlar:

- Ağ topolojisine hakim olunmalı ve sahtecilik önlemlerinin hangi cihazlarda alınabileceği belirlenmeli,
- Kullanılabilecek uRPF, ACL gibi etkin çözümler değerlendirilmeli,
- Yapılandırma hazırlanarak uygulanmalı,
- Kontrolü yapılarak korumanın sağlandığı görülmeli, kalıcı olması sağlanmalı ve güncel tutulmalıdır.

MANRS katılımcıları tarafından yapılması zorunlu eylemler:

- Kaynak adres doğrulamayı, tek bağlantılı arka uçlarına, kendi son kullanıcı ağlarına ve altyapısına uygulamalıdır.
- Yanlış kaynak adresi olan paketlerin ağa giriş çıkışını engellemek için sahtecilik önleme filtrelerini uygulamalıdır.



Kaynak IP adres sahteciliği, IP datagramı içinde yer alan kaynak IP adresi alanını değiştirerek, paketin başka bir IP adresinden geliyormuş gibi gösterilmesi durumudur. Yukarıdaki örnekte 192.0.2.1 istemcisi, 198.51.100.10 alıcısına gönderdiği paketin kaynak adres bilgisini değiştirerek, paket 203.0.113.1 adresinden geliyormuş gibi göstermektedir.

Yansılamalı Dağıtık Servis Dışı Bırakma - DDoS Reflection saldırıları, bu özellik kullanılarak yapılmaktadır. Yukarıdaki örnekte alıcı olan 198.51.100.10 adresinde, küresel sorgulamaya açık DNS, NTP gibi bir servisin bulunması durumunda, kendisine sorulana cevap oluşturacak ve paket içeriğindeki kaynak IP adresine cevap gönderecektir. Bu yapı, önceden ele geçirilmiş binlerce istemcinin (192.0.2.1 gibi) küresel sorgulara açık onlarca sunucuya (198.51.100.10), kaynak IP adresi aynı hedef girilerek (203.0.113.1) girilmesi durumu DDoS Reflection saldırısı olarak nitelendirilmektedir. Bu durumda, istemcilerden çıkan küçük paketler, dağıtık durumdaki sunuculara gitmekte, istemciler ve sunucular

boğulmadan, dolayısıyla hissedilmeden, hedef IP ve ağa büyük bir yük oluşturmaktadır. Geçtiğimiz yıllarda ve günümüzde halen yaşanan, hedef ağı, üst bağlantı servis sağlayıcısını hatta ülkeleri etkileyen büyük kapasiteli saldırılar bu topoloji ile oluşturulmaktadır.

Giriş filtrelemesi, bağlı ağların yanlış kaynak adresli paketlerinin geçmesini engelleyen filtreleme yöntemidir. Giriş filtrelemesi, sahteciliği önlemek için en azından İnternet Servis Sağlayıcı seviyesinde, bağlı kuruluşlar ve diğer ağlar için uygulanmalıdır. Tüm İSS lerin bu uygulamayı yapması durumunda sahtecilik büyük oranda önlenecektir. Yukarıdaki örnekte AS64500 kuruluşu, bağlı olan ağına, giriş yönünde kaynak Ip adresi 192.0.2.0/24 öneki haricini düşüren bir filtre girmesi durumunda, bu paket küresel ağa ulaşmadan engellenecektir. Bunun için ACL - Access Control List yazarak söz konusu filtreler oluşturulmalıdır.

Unicast Reverse Path Forwarding - uRPF, paket sonraki yönlendiriciye yönlendirilmeden önce geri dönüş rotası incelenerek, geçersiz olan paketlerin düşürülmesi yöntemidir. RFC 3704 ile tanımlanmış olan uRPF in dört çalışma kipi bulunmaktadır: Loose Mode, Feasible Path, VRF Mode, Strict Mode.

uRPF genellikle servis sağlayıcı ağının uç noktalarında, birden fazla dış bağlantısı olan yönlendiricilerin son kullanıcı, sunucu/istemci ağlarının bağlandığı arayüzlerinde uygulanır. Tek bağlantılı kuruluşlar için uRPF ***Strict*** kipi uygulanması önerilir. Ancak birden fazla bağlantısı olan kuruluşlar için, giden trafiğin diğer bağlantıdan dönebileceği düşünülerek ***Feasible*** kip kullanılması iyi olacaktır. uRPF, çok bağlantılı kurumların trafiklerinin gidiş - dönüş rotaları farklı olabileceği durumu göz önüne alınarak çok dikkatle uygulanmalı, uygulama sonrasında trafikte oluşabilecek düşüşler incelenmelidir.

Uygulanan sahtecilik önleme kurallarının işlevselliği, kontrollü yapılacak spoofer testleri ile doğrulanabilir. Ağın uç tarafında bu testin yapılması doğru olacaktır.

6. KOORDİNASYON

MANRS katılımcılarının ağ operatörleri arasında küresel iletişimi sağlamak amacıyla, "İletişim bilgilerinin her yerden erişilebilir şekilde yayınlanması ve güncel tutulması" eylemini gerçekleştirmesi gerekmektedir.

Yönlendirme vakalarının başarılı bir şekilde önlenmesi ve hafifletilmesi, dünya çapındaki ağ operatörleri arasında etkin operasyonel iletişime ve koordinasyona bağlıdır. Bu sebeple ağ operatörleri güncellenmiş bilgilerini, IRR gibi birden fazla veritabanında bulundurmalıdır. İstenilen iletişim bilgisi, Ağ işletim merkezi - NOC (Network Operations Center), IP aralıkları, alan adları için, 7/24 erişim ve temas noktası - POC (Point of Contact) bilgilerini barındırmalıdır. Bu bilgilerin bulunması istenilen yerler aşağıda listelenmektedir.

RIR WHOIS VERİTABANLARI

<mntner/>, <role/>, <inetnum/>, <inet6num/> nesneleri içinde yer alan person, tech-c, abuse-c gibi alanlar doldurulmalıdır. RIR veritabanlarına kayıt her birisi için ayrı olmakla beraber, hepsinde iletişim kayıt imkanı bulunmaktadır. mntner, tech-c gibi nesneler, bağlı bulunulan RIR arayüzünde kayıt edilmelidir.

IRR VERİTABANLARI

IRR veritabanlarına **aut-num, as-set, route-set** gibi nesneler tanımlanırken, tech-c alanı da doldurularak bilgi girişi yapılabilir. Ancak, **route/route6** nesneleri tech-c alanı içermemektedir, bu nesneler ile ilişkilendirmek için **remarks** alanı kullanılır.

PEERINGDB ARAYÜZÜ

Arayüz kayıt sırasında iletişim bilgilerini almaktadır. Bilgiler, ASN ve kayıt edilen diğer kaynaklar ile ilişkilendirerek küresel erişime açılabilir.

KURUM WEB SAYFASI

PeeringDB veya RIR sorgulamalarına aşina olmayan ağ operatörleri için, kurum web sayfasında iletişim formu, yönlendirme politikası gibi bilgilerin yer alması faydalı olabilir. Kurum web sayfasında, ağ işletim merkezi, destek ekibi, abuse ekibi, güvenlik ekibi gibi bilgilerin yer alması ulaşılmasını hızlandıracaktır.