

SAKARYA ÜNİVERSİTESİ
BİLGİSAYAR VE BİLİŞİM BİLİMLERİ FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

AĞ GÜVENLİĞİ DERSİ PROJE ÖDEV RAPORU

Seda Nur Eren - B201210030 1/A
seda.eren@ogr.sakarya.edu.tr

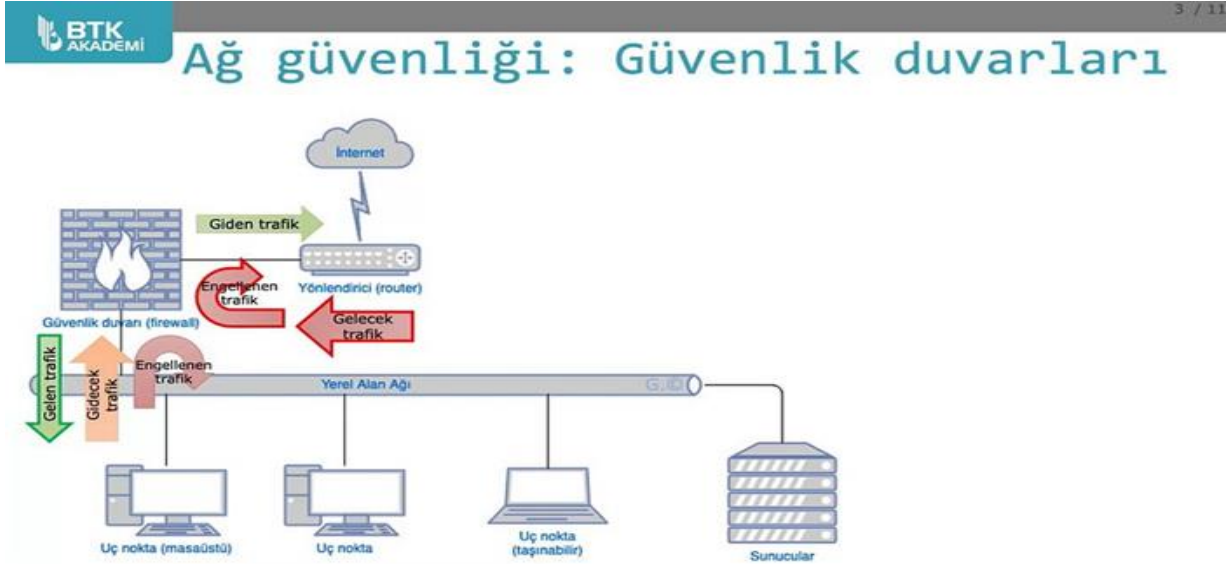
Ayşe Esra Aşcı - G201210036 1/A
ayse.asci@ogr.sakarya.edu.tr

Ödev Konusu: Güvenlik Duvarı Teknolojileri

FİREWALL

Güvenlik duvarı, özel bir ağına içine, dışına yönelik veya özel ağındaki internet trafiğini kısıtlayan bir bilgisayar ağı güvenlik sistemidir.

Bu yazılım veya özel donanım-yazılım birimi, veri paketlerini seçici olarak engelleyerek veya izin vererek çalışır. Genellikle kötü niyetli etkinliklerin önlenmesine yardımcı olmayı ve özel bir ağına içinde veya dışında herhangi birinin yetkisiz web etkinliklerine karışmasını önlemeyi amaçlar.



Nasıl çalışır ?

Ağ güvenliğinde ilk savunma hattıdır. Güvenli iç ağlar ile internet gibi güvenilir ve güvenilmeyen dış ağlar arasında bir kalkanıdır.

Network üzerinde kendisine gelen paketlerin ulaşması gereken yerlere (önceden tanımlanmış kurallarla) gidip gidemeyeceğine karar verir. Güvenlik duvarı üzerinde belirtilmiş kurallara uymayan trafiği engelleyerek koruma sağlar.

Firewall cihazlarında temel olarak beyaz liste (White List) mantığı yürütülmektedir. Kullanılan servisler, portlar ve işlemler için bir tür güvenilir liste oluşturularak izin verilmesi sağlanır. Bu listenin dışındaki tüm aktiviteler ise bloke edilerek (deny) güvenli bir ağ bağlantısı oluşturulur.

Birçok firewall, kullanıcıların istek paketlerini ağa gitmeden önce karşılayacağı bir Proxy sunucusuna sahip olabilir veya bir Proxy ile birlikte çalışabilirler.

PFSense

PfSense, FreeBSD tabanlı bir Güvenlik Duvarı (Güvenlik Duvarı) barındırmaktadır. Ücretsiz ve açık kaynak kodlara sahip olduğu için geliştirilmeye uygundur. PfSense güvenlik duvarı düşük sistem bileşenlerine sahiptir. 1 GB disk kapasitesi ve 128 MB bellek (RAM) ile bu malzeme çok rahat kullanılabilir.

Kurulumdan sonra işletim işlemleri, Pfsense için hazırlanmış olan web bölümünden yapılır. Güçlü ve esnek bir güvenlik yapıları ve dayanıklı platformun ek olarak, uzun bir özellik listesi ve paket sistemine sahip olması iyi avantaj sağlar. Güvenlik açıkları kesintilerini da engellemiyor.

Pfsense bu zamana kadar 1 Milyondan fazla kez indirilmiştir, tek bilgisayardan oluşan küçük ağlarda; binlerce ağ cihazına sahip büyük işletmelerde, üniversitelerde ve diğer organizasyonlarda sayısız kurulumla kendini kanıtlamıştır.

Pfsense ile neler yapılır?

Ağınızdaki kullanıcıların erişebilecekleri sayfaları sıkıştırabilir veya engelleyebilirsiniz.

1)Kullanıcılarınızın ziyaret ettikleri sayfaların detaylı tarih damgasıyla kayıt olabilirsiniz.[Log Kaydı]

2)Sürekli kısıtlamalar yapabilirsiniz.istediğiniz uygulamaları engelleyebilirsiniz.

3)Kategoriler belirleyerek kısıtlamaları sınırlandırır.

(Örneğin; Oyun siteleri,Forumlar,download siteleri,pornografik içerikli siteler vb.)

4)Kullanıcılarda ayrı ayrı kısıtlamalar yapılabilir.(Örneğin;öğrenciler,öğretmenler,personel,muhasebe vb.)

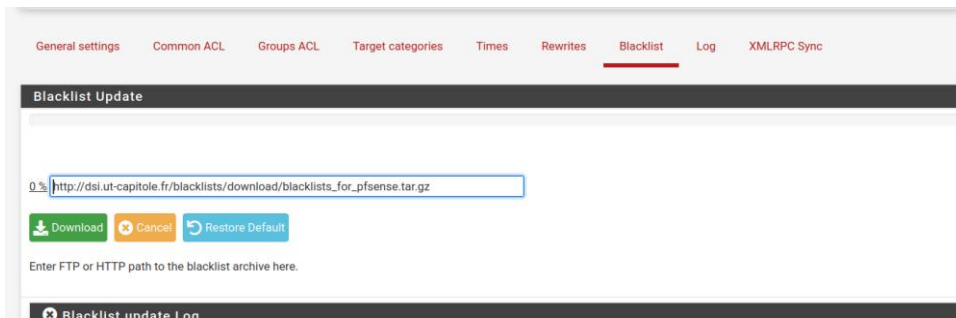
5)Kullanıcının kayıtlı kullanıcı adı ve şifre bilgileri ile internet erişimlerine izin verilebilir. Böylece wifi ağınızın şifresi korunmasa bile internete kimse erişemez.

SENARYOLAR

1)URL FİLTRELEME

URL filtreleme özelliği, pfSense'in içerik filtreleme yeteneklerini kullanarak, belirli kategorilere veya belirli anahtar kelimelere dayalı olarak web sitelerini engellemeyi sağlar. Bu sayede, ağ yöneticileri istenmeyen içeriklere karşı ağ güvenliğini artırabilir ve kullanıcıların belirli web sitelerine erişimini kontrol altında tutabilir.

Pfsense firewall tarafında yasaklamak istediğimiz HTTP protokolünü kullanan web sitelerini black list'e alıp, kullanıcıların bu web sitelerine erişmesini engelleme işlemlerini yaptık. Öncelikle BlackList'i indirdik.



Daha sonra oyun sitelerini yasaklamak için ilgili listeden games satırını deny yaptık.

[blk_blacklists_menoring]	access	---	▼
[blk_blacklists_financial]	access	---	▼
[blk_blacklists_forums]	access	---	▼
[blk_blacklists_gambling]	access	---	▼
[blk_blacklists_games]	access	deny	▼
[blk_blacklists_hacking]	access	---	▼
[blk_blacklists_jobsearch]	access	---	▼

Daha sonra Redirect mode'yi mesaj moduna alıp Proxy Denied Error kısmına kullanıcının okumasını istediğimiz mesajı yazarız . Bu işlemin sonunda oyun sitelerinde HTTP protokolünü kullanan web sitelerini yasaklamış olduk.

2)WEB SİTESİNİ ENGELLEME

PfSense üzerinde Blacklist (siyah liste) kullanarak belirli web sitelerine erişimi engelleme özelliği bulunur. Bu, ağ yöneticilerine istenmeyen içeriklere karşı koruma sağlama ve çalışanların belirli kategorilere ait web sitelerine erişimini sınırlama imkânı tanır.

Yasaklanacak olan http olan web sitelerini manuel olarak blacklist ekleyerek yeni bir kural oluşturdum.

Name	Redirect	Description
sabah	sabah.com a girişler yasaktır.	
<div>+ Add</div>		

Kuralımızı yazdıktan sonra Target Categories sayfası gelecektir. Bu sayfayı kaydedelim. Daha sonra Common ACL sekmesinden Target Rules List'i açtığımızda yazdığımız kuralın ismini göreceğiz. Deny dedikten sonra sayfayı kaydedince ilgili sayfayı engellemiş olacağız.

3)CAPTIVE PORTAL KONFIGÜRASYONU

PfSense Captive Portal, kullanıcılara ağa erişim sağlamadan önce oturum açma veya kimlik doğrulama gereksinimi olan bir özelliktir. Bu, genellikle konuk ağlarında veya kamusal Wi-Fi noktalarında kullanılır.

Öncelikle bir captive portal oluşturacağız ardından oluşturacağımız captive portalı enable yaparız.

Interfaces kısmını LAN yaparız.Maximum concurrent connections, Idle timeout (Minutes),Hard timeout (Minutes) bilgilerini güncelleriz.

Captive Portal Configuration

Enable ☒ Enable Captive Portal

Description
A description may be entered here for administrative reference (not parsed).

Interfaces

WAN

LAN

Select the interface(s) to enable for captive portal.

Maximum concurrent connections
Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.

Idle timeout (Minutes)
Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.

Hard timeout (Minutes)
Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).

Pre-authentication redirect URL : kimlik doğrulamasını geçen kullanıcıyı bir web sitesine yönlendirmek istersek burayı kullanırız.

Pre-authentication redirect URL	<input type="text"/>
<small>Set a default redirection URL. Visitors will be redirected to this URL after authentication only if the captive portal doesn't know where to redirect them. This field will be accessible through \$PORTAL_REDIRECTURLS variable in captiveportal's HTML pages.</small>	

Daha sonra Captive Portal kullanıcısı oluşturarak denetimli internet kullanımına geçtik.

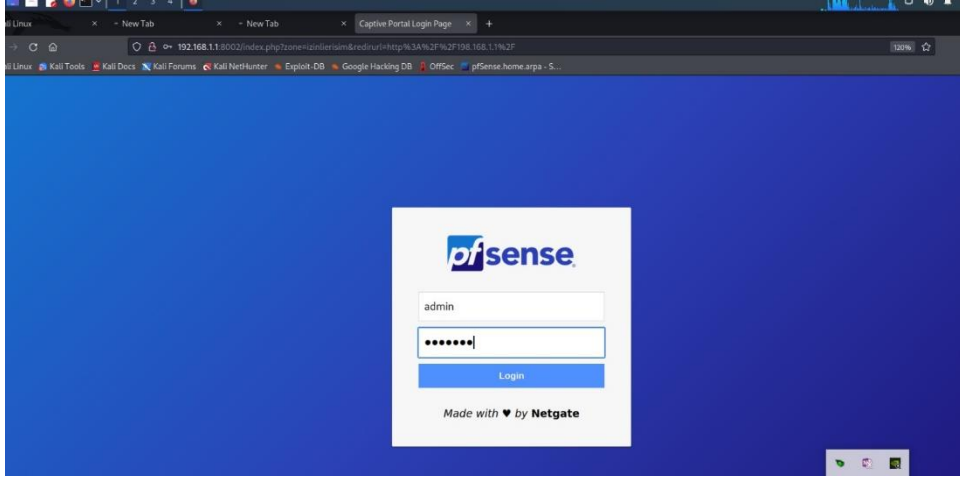
Öncelikle kullanıcı oluşturalım.

User Properties	
Defined by	USER
Disabled	<input type="checkbox"/> This user cannot login
Username	<input type="text" value="esra"/>
Password	<input type="password" value="••••••"/> <input type="password" value="••••••"/>
Full name	<input type="text" value="esra123"/> <small>User's full name, for administrative information only</small>
Expiration date	<input type="text"/> <small>Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY</small>
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.
Group membership	<div><div><input type="text"/></div><div>Not member of</div></div> <div><div><input type="text" value="admins"/></div><div>Member of</div></div>
<div>» Move to "Member of" list</div> <div>« Move to "Not member of" list</div>	

Açılan sayfadan Effective Privileges bölümündeki Add butonuna basıp. Captive Portal Login seçeneğini seçip sayfayı kaydettik.

User Privileges	
User	esra (esra123)
Assigned privileges	<div><div>System - HA node sync</div><div>User - Config: Deny Config Write</div><div>User - Notices: View</div><div>User - Notices: View and Clear</div><div>User - Services: Captive Portal login</div><div>User - System: Copy files (scp)</div><div>User - System: Copy files to home directory (chrooted scp)</div><div>User - System: Shell account access</div><div>User - System: SSH tunneling</div><div>User - VPN: IPsec xauth Dialin</div><div>User - VPN: L2TP Dialin</div><div>User - VPN: PPPoE Dialin</div><div>WebCfg - AJAX: Get Queue Stats</div><div>WebCfg - AJAX: Get Service Providers</div><div>WebCfg - AJAX: Get Stats</div><div>WebCfg - All pages</div><div>WebCfg - Crash reporter</div><div>WebCfg - Dashboard (all)</div><div>WebCfg - Dashboard widgets (direct access).</div><div>WebCfg - Diagnostics: ARP Table</div></div>

Kullanıcı bilgisayarı restart ettiğinde otomatik olarak aşağıdaki captive portal internet sayfası geliyor. Otomatik gelmezse web sayfasının URL kısmına Captive Portal Login yazarak captive portal internet sayfasına ulaşabiliriz.



4) NTOP

PfSense'in entegre bir şekilde çalışabilen araçlardan biri olan ntop, ağ trafiğini detaylı bir şekilde izleme ve analiz etme imkanı sunar. ntop, ağınız üzerindeki trafiği çeşitli parametrelerle izleyerek, hangi cihazların ne kadar veri transfer ettiğini, hangi protokollerin kullanıldığını ve bu trafiğin hangi yönlere gittiğini gösterir.

Pfsense firewall'ın detaylı network trafiğini izlemek için Pfsense firewall'a Ntop modülünün kurulumunu gerçekleştirdik.



Ntop modülünün Pfsense firewall kısmında etkin olabilmesi için gerekli ayarlamaları yaptık. Ardından Ntop web arayüzünde network trafiğine erişim sağladık.

IP Address	Flows	MAC Address	Name	Seen Since	Score	Breakdown	Throughput	Total Bytes
81.3.27.38	2	PcsCompu_D0:3F:42	community.ipfire.org	08:12		Flow: Flood	5.38 kbps ↑	41.55 KB
6.8.8.8	1	PcsCompu_D0:3F:42		08:12		Flow: Flood	234.08 kbps ↑	9.77 KB
34.149.100.209	1	PcsCompu_D0:3F:42	firefox.settings.services.mozilla.com	03:53		Flow: Flood	0 kbps ↓	5.12 KB
34.197.243.93	0	PcsCompu_D0:3F:42		01:03		Flow: Flood	0 kbps ↓	274 Bytes
208.123.73.83	1	PcsCompu_D0:3F:42		07:50		Flow: Flood	2.4 kbps ↑	31.3 KB
198.232.16.84	1	PcsCompu_D0:3F:42	tr.pinterest.com	07:23		Flow: Flood	0 kbps ↓	41.58 KB
192.168.1.2	20	PcsCompu_26:DE:4D		08:12	700	Flow: Flood	21.65 kbps ↑	14.44 MB
192.168.1.1	15	PcsCompu_D0:3F:42	pfsense.home.arpa	08:12	700	Flow: Flood	13.65 kbps ↑	14.2 MB
142.251.140.35	2	PcsCompu_D0:3F:42	www.recaptcha.net	04:34		Flow: Flood	0 kbps ↓	88.57 KB

Ntop modülüne Pfsense konsolundan 9 numaralı seçenek ile ulaştık. NTop konsol ekranından Pfsense firewall'a bağlı olan cihazların hangi ip adreslerine hangi protokol ile bağlandığını ve ne kadar veri kullandığını görmüş olduk.

```
VirtualBox Virtual Machine - Netgate Device ID: ca81feb4bf78a8b9721e
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set Interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 9
```

```
pfTop: Up State 1-22/330, View: default, Order: none, Cache: 10000 17:03:49
PR  D SRC DEST STATE AGE EXP PKTS BYTES
udp 0 ::1[62500] ::1[59633] 2:2 2201 22 211 18373
udp I ::1[62500] ::1[59633] 2:2 2201 22 211 18373
tcp 0 127.0.0.1:54447 127.0.0.1:6379 9:9 2273 52 8031 831K
tcp I 127.0.0.1:54447 127.0.0.1:6379 9:9 2273 52 8031 831K
tcp 0 127.0.0.1:44700 127.0.0.1:6379 9:9 2273 52 611 51600
tcp I 127.0.0.1:44700 127.0.0.1:6379 9:9 2273 52 611 51600
tcp 0 10.0.2.15:9333 34.107.243.93:443 4:4 2237 84164 17 3392
tcp I 192.168.1.2:58454 192.168.1.1:443 9:9 104 56 44 12521
udp 0 10.0.2.15:123 45.136.155.37:123 2:1 81 15 3 228
tcp 0 127.0.0.1:55523 127.0.0.1:953 9:9 54 36 29 9217
tcp I 127.0.0.1:55523 127.0.0.1:953 9:9 54 36 29 9217
tcp 0 127.0.0.1:59435 127.0.0.1:953 9:9 52 38 29 9217
tcp I 127.0.0.1:59435 127.0.0.1:953 9:9 52 38 29 9217
tcp 0 10.0.2.15:19749 199.7.91.13:53 9:9 52 67 11 1593
icmp 0 10.0.2.15:13317 10.0.2.2:13317 0:0 52 10 198 5742
tcp 0 10.0.2.15:51207 192.112.36.4:53 9:9 51 68 11 1605
tcp 0 10.0.2.15:4205 202.12.27.33:53 4:4 50 86376 11 2873
tcp 0 10.0.2.15:10214 193.0.14.129:53 9:9 49 68 11 1215
udp 0 ::1[22528] ::1[11571] 2:2 45 25 7 8581
udp I ::1[22528] ::1[11571] 2:2 45 25 7 8581
udp 0 ::1[6233] ::1[10520] 2:2 42 51 8 8581
udp I ::1[6233] ::1[10520] 2:2 42 51 8 8581
```

5)OPEN VPN

Öncelikle Certifica Manager' ı açıp açılan sayfada Add diyerek Descriptive name kısmına sonu .cer ile biten bir sertifika ismi verdik. Ardından Trust Store kısmındaki kutucuğu işaretleyerek oluşturulan kendinden imzalı sertifikalar windows sertifika kütüphanesinin içine otomatik olarak yerleşeceğinden OpenVPN'i her çalıştırdığımızda windows işletim sistemi bu sertifikaya güveniyor musunuz sorusunu sormayacak. Sayfanın aşağısına indigimizde Internal Certificate Authority kısmına aşağıdaki işlemleri uyguladık ;

Key type kısmına RSA altındaki seçeneğe 2048 değerini verdik.

Digest Algorithm kısmını sha512 yaparak kriptolama alanımızı daha güçlü hale getirdik.

Country Code kısmına bulunduğumuz ülkenin kodunu girdik.

State or Province kısmına bulunduğumuz ülkenin ismini girdik.




City kısmına bulunduğumuz şehrin ismini girdik.

Organization ve Organizational Unit kısmına istediğimiz bir organizasyon ismini girip sayfayı kaydettik.

Sayfayı kaydettikten sonra karşımıza gelen ekranda batuvpn.cer sertifika otoritesinin oluşmuş oldu.

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
sedavpn.cer	✓	self-signed	1	ST=TRKEY, OU=VPN-BAGLANTISI, O=VPN-BAGLANTISI, L=ISTANBUL, CN=internal-ca, C=TR Valid From: Thu, 21 Dec 2023 20:46:30 +0000 Valid Until: Sun, 18 Dec 2033 20:46:30 +0000		  

Sıradaki işlemimiz OpenVPN'in kullanacağı sertifikayı oluşturmak. Bunun için aynı sayfadaki Certificates sekmesine gelip Add/Sing dedik. Method kısmında Create an internal Certificate seçeneğini seçtik. Descriptive name kısmına sonu .ca ile biten bir isim verdik. Certificate authority, Lifetime (days) ve Key type değerlerini daha önceden oluşturduğumuz sedavpn.cer sertifika otoritesinden çekirdik. Digest Algorithm kısmını tekrardan sha512 değerini verdik. Common Name kısmına domain name verdik. Ben Pfsense sunucuma seda.local vermiştim. Bu ismi Common Name kısmına veriyorum. Certificate Type kısmını Server Certificate yaparak oluşturacağımız sertifika tipini server olarak belirleyip sayfayı kaydettik. Sayfayı kaydettikten sonra karşımıza gelen ekranda sertifikanın oluştuğunu görmüş olduk.

seoaopenvpn.ca	sedavpn.cer	ST=TRKEY, OU=VPN-BAGLANTISI, O=VPN-BAGLANTISI, L=ISTANBUL, CN=seda.local, C=TR	OpenVPN Server	  
Server Certificate				
CA: No		Valid From: Thu, 21 Dec 2023 20:47:55 +0000		
Server: Yes		Valid Until: Sun, 18 Dec 2033 20:47:55 +0000		

Açılan sayfada kimlik doğrulamasını nasıl yapılacağını soruyor. Ortamımızda Radius sunucu varsa ve biz kimlik doğrulamasını Radius üzerinde yapmak istersek RADIUS'u seçelim. Ortamımızda Active Directory varsa domain kullanıcılarını LDAP'tan çekip kimlik doğrulamasını bu şekilde yapabiliriz. Domain veya RADIUS ortamımız yoksa veya biz Pfsense sunucusunda oluşturulan local user'lar ile kimlik doğrulaması yapmak istersek Local User Access seçeneğini seçmemiz gerekmektedir. Biz bu seçeneği seçip devam ettik. Daha önceden oluşturduğumuz sertifika otoritesini seçip devam ettik. Daha son sayfadaki işlemleri de yaptık ve Sayfanın aşağısına indiğimizde Tunnel Settings ayalarını yapalım.




Tunnel Network kısmı kullanıcılar VPN ile bizim sistemimize bağlandığında bu kısma verdiğimiz ip adresi üzerinde bir DHCP havuzu oluşur ve VPN ile bağlantı sağlayan kullanıcılar oluşturulan bu havuzdan kendilerine ip adresi alır.

Redirect Gateway kısmındaki kutucuğu işaretlediğimizde (Full Tunnel) VPN ile ağımıza bağlanan kullanıcı internet kullanımını şirket internetini kullanarak yapacaktır. Böylece kullanıcının internet log'unu tutmuş oluruz. Bu kutucuğu işaretlemesek (Split Tunnel) kullanıcı VPN ile şirket ağımıza bağlanır kullanması gereken kaynakları kullanır fakat interneti kullanmak isterse kendi bulunduğu fiziksel ortamdaki internet ağını kullanır. Böylece şirket internet bandını kullandırmamış oluruz. Local Network kısmına Pfsense firewall tarafında kullandığım local ip adresini giriyorum.

Concurrent Connections kısmına aynı anda kaç kullanıcının bağlanmasını istiyorsak buradan kısıtlama yapabiliriz.

OpenVPN rule kısmı daha sonradan oluşturduğumuz VPN kullanıcılarına kısıtlama yapmak istersek ihtiyaç duyacağımız menü arayüzünü firewall tarafına ekler.

Karşımıza gelen sayfada OpenVPN ayarlarının tamamlandığını görmüş olduk.

OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	236.125.12.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA512 D-H Params: 2048 bits	OpenVPN	  

6)LOGLAMA





PfSense üzerindeki günlükler (logs), ağ üzerinden geçen trafiği, güvenlik olaylarını ve diğer önemli bilgileri kaydeder. Bu günlükler, ağdaki kullanıcıların internete erişimini, ziyaret ettikleri siteleri, kullanılan protokolleri ve daha birçok bilgiyi içerebilir.

Loglama işlemi için ilk olarak gerekli olan paket yüklemesini gerçekleştirdik. Kurulumun ardından gerekli işlemleri Squid Proxy Report kısmında yaptık.

System / Package Manager / Installed Packages

Installed PackagesAvailable Packages

Installed Packages

Name	Category	Version	Description	Actions
✓ Lightsquid	www	3.0.7.3	Lightsquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package.	 
Package Dependencies:				
 lighttpd-1.4.72  lightsquid-1.8.5				

Raporlama web sayfasına erişim sağladık. Bu kısımda kullanıcının nereye gittiğini öğrenmiş olduk.

https://192.168.1.17445					
Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec pfSense.home.arpa - S...					
Squid user access report					
Work Period: Dec 2023					
Calendar			Top Sites		
2023			Total		
01 02 03 04 05 06 07 08 09 10 11 12			YEAR YEAR YEAR		
			MONTH MONTH MONTH		
Date	Group	Users	OverSize	Bytes	Average Hit %
20 Dec 2023	grp	2	0	112 338	56 169 0.00%
Total/Average:		2	0	112 338	56 169 0.00%
LightSquid v1.8 (c) Sergey Erokhin AKA ESI					

Grp kısmı ile clientlerin listesini görebildik. İnternette bulunan client ip adresi aşağıda görülmektedir.

Squid user access report						
Date: 20 Dec 2023 (update :: 16:40 :: 20 Dec 2023)						
Top Sites Report						
Big Files Report						
#	Time	User	Real Name	Connect	Bytes	%
00	no in group					
1		192.168.1.2	Sergey Erokhin	19	90 563	80.6%
2		127.0.0.1	?	5	21 775	19.3%
				112 338	100.0%	

#	Group	Bytes	%
1	00_no in group	112 338	100.0

LightSquid v1.8 (c) Sergey Erokhin AKA ESL

Saat ikonunu kullanarak saat bazlı raporlama sayfasına ulaşıyoruz.

Squid user access report						
User: 192.168.1.2 (Sergey Erokhin)						
Date: 20 Dec 2023						
#	Accessed site	00	01	02	03	04
Total		01	02	03	04	05
1	192.168.1.1	01	02	03	04	05
2	www.007arcadegames.com	01	02	03	04	05
Total		01	02	03	04	05

LightSquid v1.8 (c) Sergey Erokhin AKA ESL

Top sites en çok ziyaret edilen sitelerin sayfası.

Squid user access report				
Top Sites				
Work Period: 20 Dec 2023				
#	Accessed site	Connect	Bytes	%
1	who 192.168.1.1	23	112 338	100.0%
2	who www.007arcadegames.com	1	0	0.0%
Total		112 338		

LightSquid v1.8 (c) Sergey Erokhin AKA ESL

7)SSH etkinleştirme

Öncelikle Secure shell' e izin verdik.

Secure Shell

Secure Shell Server

☒ Enable Secure Shell

SSHd Key Only

Password or Public Key

When set to **Public Key Only**, SSH access requires authorized keys and these keys must be configured for each **user** that has been granted secure shell access. If set to **Require Both Password and Public Key**, the SSH daemon requires both authorized keys and valid passwords to gain access. The default **Password or Public Key** setting allows either a valid password or a valid authorized key to login.

Allow Agent Forwarding

☐ Enables ssh-agent forwarding support.

SSH port

22

Note: Leave this blank for the default of 22.

Daha sonra Güvenlik Duvarı kuralı oluşturma ekranında aşağıdaki yapılandırmayı gerçekleştirdik:

- Eylem - Geçiş
- Arayüz - WAN
- Adres ailesi - IPV4
- Protokol - TCP

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

WAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Burada, Pfsense güvenlik duvarından tüm hizmetlerin durumunu doğrulayabiliriz. Örneğimizde SSH hizmeti etkin ve çalışıyor.

Status / Services

Services			
Service	Description	Status	Actions
c-icap	ICAP Interface for Squid and ClamAV integration	✗	▶
captiveportal	Captive Portal: izinlerisim	✓	🔄 ⚙️ 📊 📋
clamd	ClamAV Antivirus	✗	▶
dhcpd	ISC DHCP Server	✓	🔄 ⚙️ 📊 📋
dpinger	Gateway Monitoring Daemon	✓	🔄 ⚙️ 📊 📋
lightsquid_web	Lightsquid Web Server	✓	🔄 ⚙️
ntopng	ntopng Network Traffic Monitor	✓	🔄 ⚙️
ntpd	NTP clock sync	✓	🔄 ⚙️ 📊 📋
openvpn	OpenVPN server: OpenVPN	✓	🔄 ⚙️ 📊 📋
squid	Squid Proxy Server Service	✓	🔄 ⚙️ 📊 📋
squidGuard	Proxy server filter Service	✓	🔄 ⚙️
sshd	Secure Shell Daemon	✓	🔄 ⚙️
syslogd	System Logger Daemon	✓	🔄 ⚙️ 📊 📋
unbound	DNS Resolver	✓	🔄 ⚙️ 📊 📋

Varsayılan olarak PfSense güvenlik duvarı, WAN arayüzüne harici SSH bağlantılarına izin vermez.

Örneğimizde SSH iletişimine izin vermek için bir güvenlik duvarı kuralı oluşturacağız.

Kuralları aşağıdaki gibi oluşturduk.

Source

Source

☐ Invert match

Any

Source Address

/

⚙️ Display Advanced

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must n its default value, any.

Destination

Destination

☐ Invert match

WAN address

Destination Address

/

Destination Port Range

SSH (22)

From

Custom

To

SSH (22)

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog serv the Status: System Logs: Settings page).

Description

SSH on WAN

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the fi log.

Advanced Options

⚙️ Display Advanced

Kaydet düğmesine tıkladığınızda Güvenlik Duvarı yapılandırma ekranına geri yönlendirileceksiniz.

Şimdi SSH yapılandırmasını uygulamak için güvenlik duvarı kurallarını yeniden yükledik ve ardından

güvenlik duvarı yapılandırmasını da yeniden yükledik.

The screenshot shows the 'Source' and 'Destination' tabs of a firewall rule configuration. The 'Source' tab is active, showing 'Source Address' as 'Any'. The 'Destination' tab is also visible, showing 'Destination Address' as 'WAN address' and 'Destination Port Range' as 'SSH (22)'. The 'Extra Options' section is expanded, showing 'Log' checked and 'Description' as 'SSH on WAN'. The 'Advanced Options' section is also visible at the bottom.

Daha sonra Pfsense SSH iletişimini test etmek için aşağıdaki komutları kullandık.

The screenshot shows the 'PuTTY Configuration' window. The 'Category' list on the left includes 'Session', 'Logging', 'Terminal', 'Keyboard', 'Bell', 'Features', 'Window', 'Appearance', 'Behaviour', 'Translation', 'Selection', 'Colours', 'Connection', 'Data', 'Proxy', 'SSH', 'Serial', 'Telnet', 'Rlogin', and 'SUPDUP'. The 'SSH' category is selected. The 'Basic options for your PuTTY session' section shows 'Host Name (or IP address)' as '192.168.1.1' and 'Port' as '22'. The 'Connection type' is set to 'SSH'. The 'Load, save or delete a stored session' section shows 'Saved Sessions' and 'Default Settings' with 'Load', 'Save', and 'Delete' buttons. The 'Close window on exit' section has 'Only on clean exit' selected. The 'Open' button is highlighted.

Ve böylece Pfsense SSH iletişim testini yaptık.

8) Pfsense SNMP Yapılandırması

PfSense üzerinde gerçekleştirdiğim SNMP yapılandırması, ağ yöneticilerine PfSense güvenlik duvarı üzerindeki önemli bilgileri izleme ve analiz etme imkanı tanıyan bir süreci içerir. Bu yapılandırma sayesinde, SNMP (Simple Network Management Protocol) aracılığıyla ağ cihazlarının performansı, trafiği ve durumu gibi önemli verilere erişim sağlanabilir.

Burada SNMP'ye ait bir kişi oluşturup bilgilerini girdik.

Gerekli olan modülleri seçildi. Arayüz bağlantı yapılandırılması için tümünü seçtik.

SNMP Daemon
Enable ☒ Enable the SNMP Daemon and its controls

SNMP Daemon Settings
Polling Port
Enter the port to accept polling events on (default 161).
System Location
System Contact
Read Community String
The community string is like a password, restricting access to querying SNMP to hosts knowing the community string. Use a strong value here to protect from unauthorized information disclosure.

SNMP Traps Enable
Enable ☐ Enable the SNMP Trap and its controls

SNMP Modules
SNMP modules ☒ MibII
☒ Netgraph
☒ PF
☒ Host Resources
☒ UCD
☒ Regex

Interface Binding
Internet Protocol
Bind Interfaces ☒ All
☐ WAN
☐ LAN
☐ Localhost

Pfsense güvenlik duvarı WAN arayüzünde harici SNMP bağlantılarına izin vermez. İzin verebilmesi için güvenlik duvarı kuralı oluşturduk. Pfsense güvenlik duvarı ile SNMP iletişimi gerçekleştirmesine izin verilmesi gereken IP adresini tanımlamak gerekir. Herhangi bir bilgisayara ait güvenlik duvarı ile SNMP iletişimi gerçekleştirebilecek şekilde ayarladık.

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✗	0/0 B	*	RFC 1918 networks	*	*	*	*	*	Block private networks	
<input checked="" type="checkbox"/>	✗	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	Block bogon networks	
<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	*	*	WAN address	161 (SNMP)	*	none	SNMP on WAN	

Pfsense SNMP yapılandırmasını Linux ortamında test ettik.

```
(kali@kali)~$ apt-get install snmp
snmpd will be installed as public 192.168.1.1
E: Could not open lock file /var/lib/dpkg/lock-frontent - open (13: Permission denied)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontent), are you root?
iso.3.6.1.2.1.1.1.0 = STRING: "pfsense pfsense.home.arpa 2.7.2-RELEASE FreeBSD 14.0-CURRENT amd64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.12225.1.1.2.1.1
iso.3.6.1.2.1.1.3.0 = Timeticks: (39310) 0:06:33.10
iso.3.6.1.2.1.1.4.0 = STRING: "esra"
iso.3.6.1.2.1.1.5.0 = STRING: "pfsense.home.arpa"
iso.3.6.1.2.1.1.6.0 = STRING: "Room"
iso.3.6.1.2.1.1.7.0 = INTEGER: 76
iso.3.6.1.2.1.1.8.0 = Timeticks: (16) 0:00:00.16
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.4.1.12325.1.1.1.10.2 Rules / WAN
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.4.1.12325.1.1.1.10.3
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.4.1.12325.1.1.1.10.4
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.4.1.12325.1.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.31
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.48
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.2.1.4.24
iso.3.6.1.2.1.1.9.1.2.11 = OID: iso.3.6.1.4.1.12325.1.2 Status Protocol Source Port Destination Port Gateway Queue Size
iso.3.6.1.2.1.1.9.1.2.12 = OID: iso.3.6.1.2.1.25
iso.3.6.1.2.1.1.9.1.2.13 = OID: iso.3.6.1.4.1.2021
iso.3.6.1.2.1.1.9.1.2.14 = OID: iso.3.6.1.4.1.12325.1.203
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "udp transport mapping"
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "isock transport mapping"
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "inet transport mapping"
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities."
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "The MIB module for the Begetot-SNMPd."
iso.3.6.1.2.1.1.9.1.3.6 = STRING: "The MIB module to describe generic objects for network interface sub-layers."
iso.3.6.1.2.1.1.9.1.3.7 = STRING: "The MIB module for managing IP and ICMP implementations, but excluding their management of IP routes."
iso.3.6.1.2.1.1.9.1.3.8 = STRING: "The MIB module for managing TCP implementations."
iso.3.6.1.2.1.1.9.1.3.9 = STRING: "The MIB module for managing UDP implementations."
iso.3.6.1.2.1.1.9.1.3.10 = STRING: "The MIB module for the display of CIDR multipath IP Routes."
iso.3.6.1.2.1.1.9.1.3.11 = STRING: "The MIB for the NetGraph access module for SNMP."
iso.3.6.1.2.1.1.9.1.3.12 = STRING: "The MIB module for Host Resource MIB (RFC 2798)."
iso.3.6.1.2.1.1.9.1.3.13 = STRING: "The MIB module for UCD-SNMP-MIB."
iso.3.6.1.2.1.1.9.1.3.14 = STRING: "The MIB for regex data."
iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.5 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.6 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.7 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.8 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.9 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.10 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.11 = Timeticks: (15) 0:00:00.15
iso.3.6.1.2.1.1.9.1.4.12 = Timeticks: (15) 0:00:00.15
```

```
iso.3.6.1.2.1.31.1.2.1.3.0.4 = INTEGER: 1
iso.3.6.1.2.1.31.1.2.1.3.0.5 = INTEGER: 1
iso.3.6.1.2.1.31.1.2.1.3.0.6 = INTEGER: 1
iso.3.6.1.2.1.31.1.2.1.3.0.7 = INTEGER: 1
iso.3.6.1.2.1.31.1.2.1.3.1.0 = INTEGER: 1
iso.3.6.1.2.1.31.1.2.1.3.2.0 = INTEGER: 1
iso.3.6.1.2.1.31.1.2.1.3.3.0 = INTEGER: 1
iso.3.6.1.2.1.31.1.2.1.3.4.0 = INTEGER: 1
iso.3.6.1.2.1.31.1.2.1.3.5.0 = INTEGER: 1
iso.3.6.1.2.1.31.1.2.1.3.6.0 = INTEGER: 1
iso.3.6.1.2.1.31.1.2.1.3.7.0 = INTEGER: 1
iso.3.6.1.2.1.31.1.4.1.2.1.6.1.0.94.0.0.1 = INTEGER: 1
iso.3.6.1.2.1.31.1.4.1.2.1.6.8.0.39.180.140.87 = INTEGER: 1
iso.3.6.1.2.1.31.1.4.1.2.1.6.51.51.0.0.0.1 = INTEGER: 1
iso.3.6.1.2.1.31.1.4.1.2.1.6.51.51.24.97.32.206 = INTEGER: 1
iso.3.6.1.2.1.31.1.4.1.2.1.6.51.51.255.24.97.32 = INTEGER: 1
iso.3.6.1.2.1.31.1.4.1.2.1.6.51.51.255.180.140.87 = INTEGER: 1
iso.3.6.1.2.1.31.1.4.1.2.1.6.255.255.255.255.255.255 = INTEGER: 1
iso.3.6.1.2.1.31.1.4.1.2.2.6.1.0.94.0.0.1 = INTEGER: 1
iso.3.6.1.2.1.31.1.4.1.2.2.6.8.0.39.236.115.173 = INTEGER: 1
iso.3.6.1.2.1.31.1.4.1.2.2.6.51.51.0.0.0.1 = INTEGER: 1
iso.3.6.1.2.1.31.1.4.1.2.2.6.51.51.0.0.0.2 = INTEGER: 1
iso.3.6.1.2.1.31.1.4.1.2.2.6.51.51.24.97.32.206 = INTEGER: 1
iso.3.6.1.2.1.31.1.4.1.2.2.6.51.51.255.1.0.1 = INTEGER: 1
iso.3.6.1.2.1.31.1.4.1.2.2.6.51.51.255.24.97.32 = INTEGER: 1
iso.3.6.1.2.1.31.1.4.1.2.2.6.51.51.255.236.115.173 = INTEGER: 1
iso.3.6.1.2.1.31.1.4.1.2.2.6.255.255.255.255.255.255 = INTEGER: 1
iso.3.6.1.2.1.31.1.4.1.2.3.6.8.0.39.100.164.241 = INTEGER: 1
iso.3.6.1.2.1.31.1.4.1.2.3.6.255.255.255.255.255.255 = INTEGER: 1
iso.3.6.1.2.1.31.1.4.1.3.1.6.1.0.94.0.0.1 = INTEGER: 2
iso.3.6.1.2.1.31.1.4.1.3.1.6.8.0.39.180.140.87 = INTEGER: 3
iso.3.6.1.2.1.31.1.4.1.3.1.6.51.51.0.0.0.1 = INTEGER: 2
iso.3.6.1.2.1.31.1.4.1.3.1.6.51.51.24.97.32.206 = INTEGER: 2
iso.3.6.1.2.1.31.1.4.1.3.1.6.51.51.255.24.97.32 = INTEGER: 2
iso.3.6.1.2.1.31.1.4.1.3.1.6.51.51.255.180.140.87 = INTEGER: 2
iso.3.6.1.2.1.31.1.4.1.3.1.6.255.255.255.255.255.255 = INTEGER: 3
iso.3.6.1.2.1.31.1.4.1.3.2.6.1.0.94.0.0.1 = INTEGER: 2
iso.3.6.1.2.1.31.1.4.1.3.2.6.8.0.39.236.115.173 = INTEGER: 3
iso.3.6.1.2.1.31.1.4.1.3.2.6.51.51.0.0.0.1 = INTEGER: 2
iso.3.6.1.2.1.31.1.4.1.3.2.6.51.51.0.0.0.2 = INTEGER: 2
iso.3.6.1.2.1.31.1.4.1.3.2.6.51.51.24.97.32.206 = INTEGER: 2
iso.3.6.1.2.1.31.1.4.1.3.2.6.51.51.255.1.0.1 = INTEGER: 2
iso.3.6.1.2.1.31.1.4.1.3.2.6.51.51.255.24.97.32 = INTEGER: 2
iso.3.6.1.2.1.31.1.4.1.3.2.6.51.51.255.236.115.173 = INTEGER: 2
iso.3.6.1.2.1.31.1.4.1.3.2.6.255.255.255.255.255.255 = INTEGER: 3
iso.3.6.1.2.1.31.1.4.1.3.3.6.8.0.39.100.164.241 = INTEGER: 3
iso.3.6.1.2.1.31.1.4.1.3.3.6.255.255.255.255.255.255 = INTEGER: 3
iso.3.6.1.2.1.31.1.5.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.31.1.6.0 = Timeticks: (0) 0:00:00.00
```