# CYBERWISE PROFESYONEL SERVİSLER
# LAB NOTLARI

Certified Professional Services Partner


**Temmuz 2022** ps-info@cyberwise.com.tr

CYBER WISE

PROFESYONELSERVİSLER

# LAB NOTLARI

CHECK POINT

- Generic Data Center Obje Özelliği
- NAT Rule Number 0 açıklaması
- SecureXL Fast Accelerator Özelliği

05 Temmuz 2022

# Generic Data Center Obje Özelliği

Generic Data Center özelliği, external web server veya smartcenter makinesinde bulunan JSON dosyalarında tanımlanan IP adreslerine erişimleri kontrol etme yeteneği sağlar.

Generic Data Center objesi, JSON dosyası her değiştiğinde Security Gateway tarafında otomatik olarak güncellenir.
Güncellemelerin etkili olması için policy installation işlemine gerek yoktur.
Bu dosyalara dayalı olarak oluşturulan nesneler, aşağıdaki politikalarda source veya destination olarak kullanılabilir:
**Access Control policy, NAT policy, Threat Prevention policy, HTTPS Inspection policy.**

**Policy install etmeden dinamik kaynaklardan firewall kuralının yönetilmesi sağlanır.**

- Sadece R81.x serisinde desteklenir.
- IPv4 ve IPv6 adresler desteklenir.

Generic Data Center obje tanımını kullanabilmek için ilk aşamada bir JSON dosyası oluşturacağız.

# Generic Data Center Obje Özelliği JSON File Structure

- Currently, only version 1.0 is supported.
- The "id" field should be a **unique UID**.
- **Mandatory fields:** "version", "objects", "name", "id", "ranges".

## Örnek JSON File Structure

```
{
    "version": "1.0",
    "description": "Generic Data Center file example",
    "objects": [
                {
                    "name": "Object A name",
                    "id": "e7f18b60-f22d-4f42-8dc2-050490ecf6d5",
                    "description": "Example for IPv4 addresses",
                    "ranges": [
                                "91.198.174.192",
                                "20.0.0.0/24",
                                "10.1.1.2-10.1.1.10"
                    ]
                },
                {
                    "name": "Object B name",
                    "id": "a46f02e6-af56-48d2-8bfb-f9e8738f2bd0",
                    "description": "Example for IPv6 addresses",
                    "ranges": [
                                "2001:0db8:85a3:0000:0000:8a2e:0370:7334",
                                "0064:ff9b:0000:0000:0000:0000:1234:5678/96",
                                "2001:0db8:85a3:0000:0000:8a2e:2020:0-2001:0db8:85a3:0000:0000:8a2e:2020:5"
                    ]
                }
    ]
}
```

# Generic Data Center Obje Özelliği

## LAB Örneği için JSON Dosya içeriği

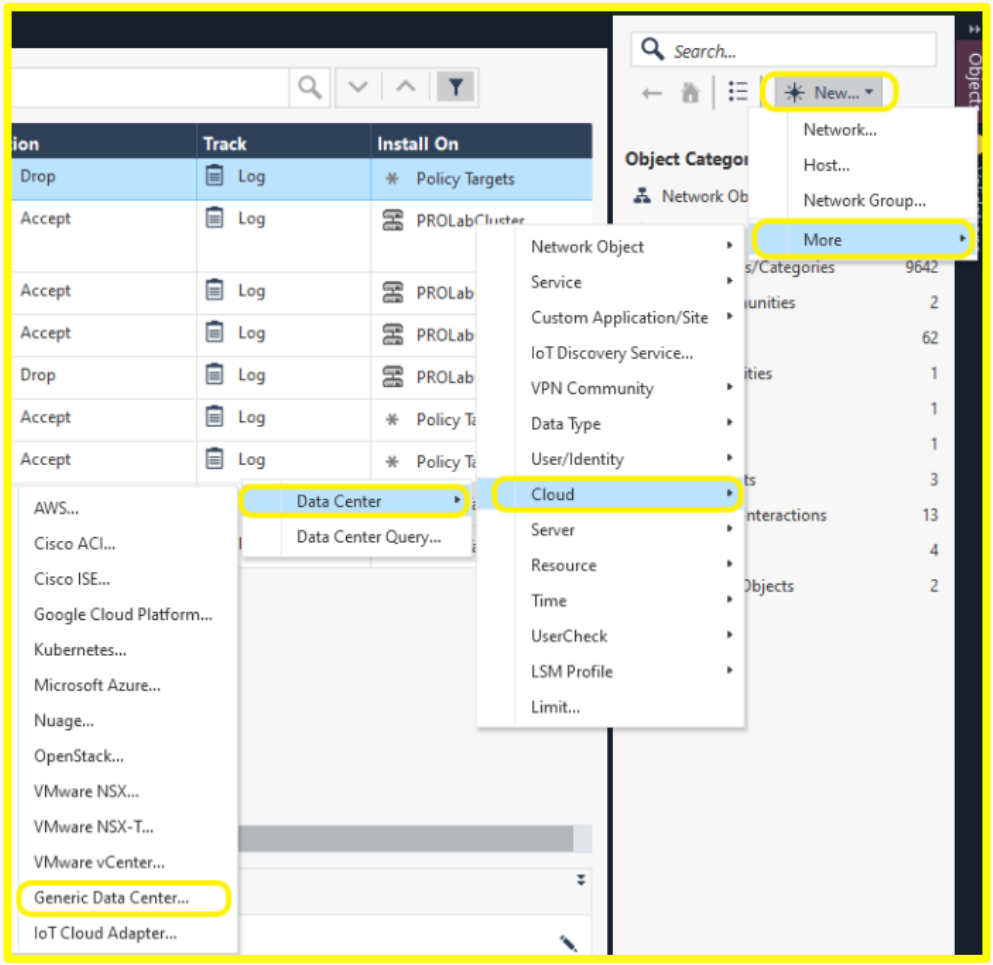
Örneğimizde iki adet ip adresi kullanıldı ve bunlar google.com sitesine ait.Dosya GenericDC.json ismi ile kayıt edildi.Bu dosyayı SmartCenter üzerinde tmp altına transfer ediyoruz. /tmp/GenericDC.json

```
{
    "version": "1.0",
    "description": "Generic Data Center LAB Test",
    "objects": [
                {
                    "name": "IP List A",
                    "id": "e7f18b60-f22d-4f42-8dc2-050490ecf6d5",
                    "description": "IPv4 Listesi",
                    "ranges": [
                                "172.253.123.105",
                                "172.253.123.106"
                    ]
                },
                {
                     "name": "IP List B",
                     "id": "a46f02e6-af56-48d2-8bfb-f9e8738f2bd0",
                     "description": "IPv6 Listesi",
                     "ranges": [
                                "2001:0db8:85a3:0000:0000:8a2e:0370:7334",
                                "0064:ff9b:0000:0000:0000:0000:1234:5678/96"
                     ]
                }
   ]
}
```

# Generic Data Center Obje Özelliği

## Generic Data Center Objesinin oluşturulması

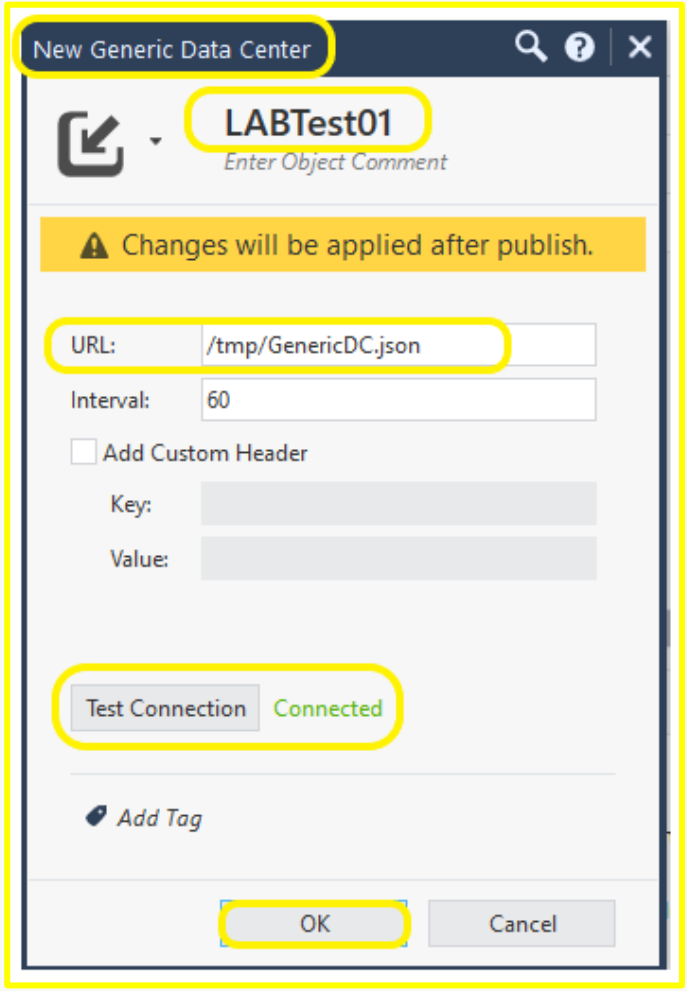
SmartConsole üzerinde **New > More > Cloud > Data Center > Generic Data Center** seçimi ile yeni bir obje oluşturuyoruz.



# Generic Data Center Obje Özelliği

## Generic Data Center Objesinin oluşturulması

Obje name kısmına **LABTest01** yazabiliriz. Json dosyasını SmartCenter üzerine transfer etmiştik.Bu alanın dizin bilgisini yazıyoruz.
Test Connection butonu ile bağlantının durumunu teyit ediyoruz.Sonrasında publish ile işlem tamamlanıyor.



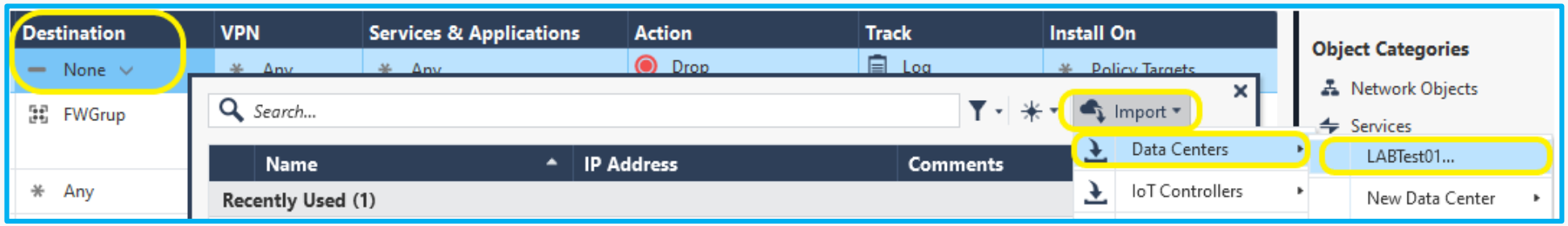

**JSON dosyasını SmartCenter üzerinde local feed olarak gösterebiliriz.**
Örnek: **/tmp/file.json**

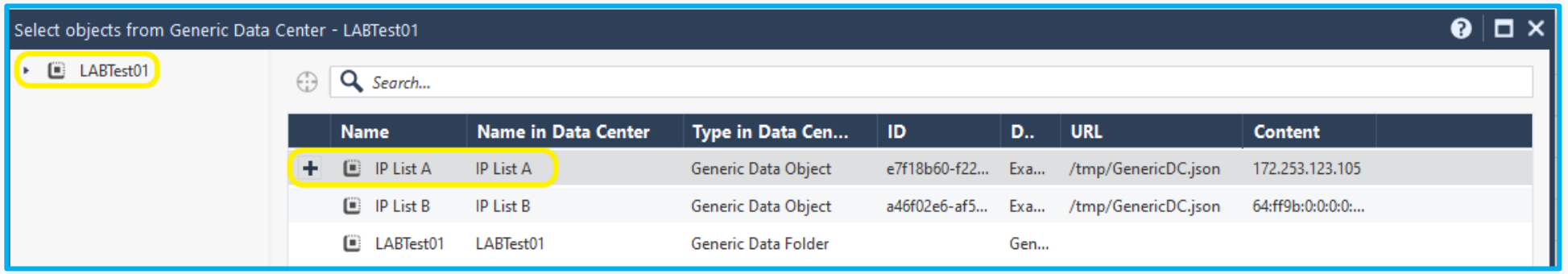
**Veya Remote feed olarak ilgili url bilgisini tanımlayabiliriz.**
Örnek: **https://example.com/file.json (remote feed)**

Eğer remote feed bir **HTTPS bağlantısı** üzerinden tanımlandıysa **server sertifika** bilgisini elde etmeniz gerekmektedir.

# Generic Data Center Obje Özelliği Generic Data Center Objesinin kuralda kullanılması

Bu örnekte **Source: TestPC Destination** ise **Generic Data Center objesi** olacak.
**Amacımız;**TestPC üzerinden yapılan isteklerde Generic Data Center objesine bağlı ip adresleri varsa bunların engellenmesi.Destination kısmına aşağıdaki şekilde daha önceden tanımladığımız Generic Data Center objesini ekliyoruz.Açılan pencerede **ipv4 adreslerinin yer aldığı IP List A seçiyoruz.**
Tanımlar sonrası kuralımız aşağıdaki şekilde oluşacaktır.

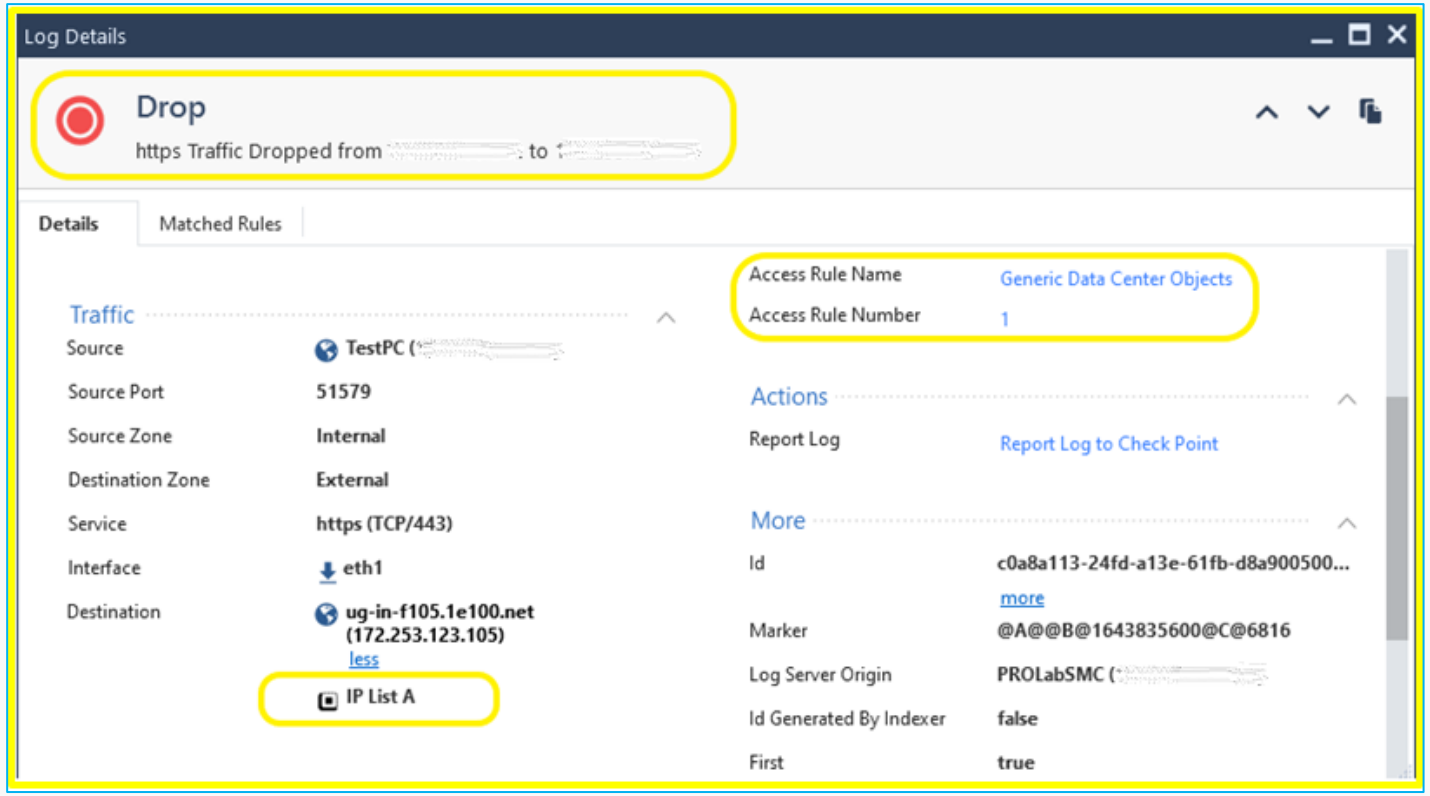



## Test Sonuçları

Test PC üzerinden 172.253.123.105 ip adresine doğru yapılan istek Generic Data Center Objesinin yer aldığı kural nedeniyle engellendi.

**Not:**Doğru kod yazımı ile oluşturulmuş JSON dosyası devreye alındıktan sonra JSON dosyası içerisinde yapılacak ikinci güncellemede kod yanlış yazılırsa generic data center objesi ile oluşturulan ilk ve geçerli JSON dosyası çalışmaya devam edecektir.Hatalı kod geçerli olmayacaktır.



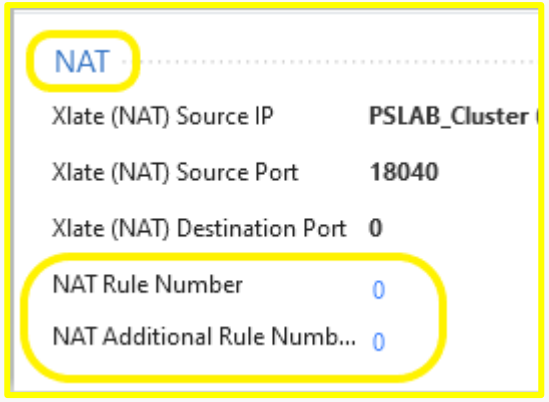
# NAT Rule Number 0 ve Implied Rule Tanımları

SmartLog üzerinde log kayıtlarını incelediğimizde bazı loglarda NAT Rule Number 0 bilgisi yer alır.
Bu durum firewall üzerinde fabrika ayarları ile birlikte gelen Implied Rule mekanizmasının çalışma yapısı ile ilgilidir.

**NAT Rule Number 0** loglarının oluşumu ile ilgili LAB ortamımızda bazı denemeler yaptık.

Trafiği oluşturan source host veya network kaynağı ile ilgili NAT kural tablosunda bir tanım yoksa Implied Rule tablosu ile eşleşen trafik NAT Rule Number 0 olarak log kayıtlarında yer almaktadır.
Çünkü Implied Rule için bir kural numarası atanmaz ve bu kayıt 0 rakamı ile gösterilir.

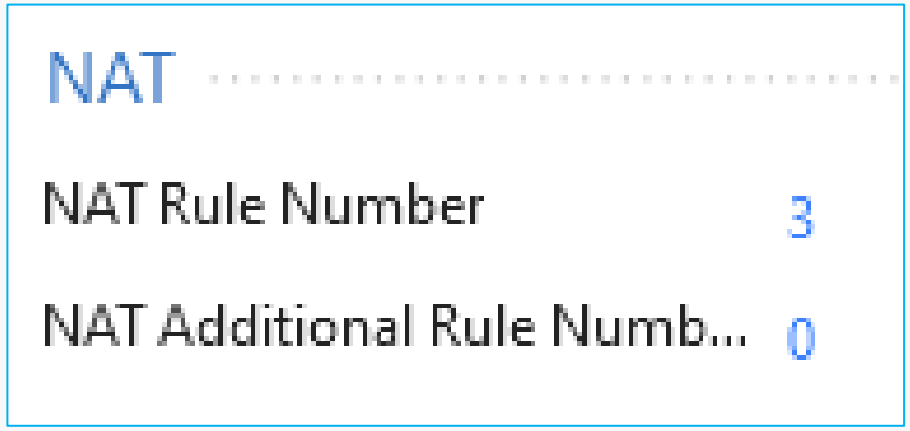
**Örnek olarak;**
Cluster Aktif member üzerinden internet erişimleri (firewallun kendini source olarak göstermesi)
Cluster Standby member sync portu üzerinden gerçekleşen aktif member bağlantıları



# NAT Rule Number 0 ve Implied Rule Tanımları

## NAT Additional Rule Number 0

Trafik bir adet otomatik NAT kuralı ile eşleşir ise bu kayıt 0 olarak loglanır.
Eğer iki otomatik NAT rule ile trafik eşleşir ise (source ve diğeri destination olmak üzere) ikinci kural numarası bu alanda yer alır.




### Managing the Firewall Rule Base

Use SmartDashboard to easily create and configure Firewall rules for a strong security policy.

These are the fields that manage the rules for the Firewall security policy.

| Field | Description |
|---|---|
| No. | Rule number in the Firewall Rule Base. Implied rules do not have a number. |

# SecureXL Fast Accelerator Özelliği

SecureXL Fast Accelerator **(fw fast_accel)** ile güvenilir bağlantıların deep packet inspection modülüne sokulmadan hedef noktaya ulaşması sağlanır.
Bu sayede CPU kullanımlarında düşüş sağlanabilinir.Güvenilir bağlantılar ile performans kazanımı elde etmek istiyorsak bu özelliği değerlendirebiliriz.
Özellikle SecureXL **medium path** üzerinden kontrol edilen bağlantılarda etkili olmaktadır.

**Bu özelliğin nitelikleri;**

- Configured from the gateway's CLI.
- Can be turned On / Off, **Off is the default.**
- Rules can be added (up to 24) / deleted by demand.
- Configuration (State / rules) **survive reboot.**
- Maintain rule hit count (does not survive reboot).
- Every configuration change done by the user is logged in $FWDIR/log/fw_fast_accel.log file.
- Upon connection acceleration a log is sent to the management.

# SecureXL Fast Accelerator Özelliği

## Kullanım Seçenekleri ve Örnekler

```
Options:
        add             - Add fast_accel rule
        delete          - Delete fast_accel rule
        delete_all      - Delete all fast_accel rules
        enable          - Set feature state to on
        disable         - Set feature state to off
        show_table      - Display the configured rules
        show_state      - Display the current feature state
        reset_stats     - Reset the collected statistics
        export_conf     - Export fast_accel configuration
        import_conf     - Import fast_accel configuration
        -h              - Display this help message
```

```
Example Usage:
        fw  ctl fast_accel add 1.1.1.1 2.2.2.0/24 80 6
        fw  ctl fast_accel delete 192.168.0.0/16 any 16 17
        fw  ctl fast_accel add 255.0.0.0/8 255.240.0.0/12 16 any
        fw6 ctl fast_accel add 2620::/16 1155:5A6B::/32 80 any
        fw6 ctl fast_accel show_table
        fw  ctl fast_accel enable
        fw  ctl fast_accel disable
        fw  ctl fast_accel show_state
        fw  ctl fast_accel export_conf
        fw  ctl fast_accel import_conf
        fw  ctl fast_accel delete_all
```

```
Add/Delete Rule Specifications:
        Usage: fw ctl fast_accel <add/delete> <source address> <destination address> <destination port> <protocol>
        Each rule must contain the following parameters:
        1) source address          <source ip>/<subnet>        - Subnet is optional.
        2) destination address     <destination ip>/<subnet>   - Subnet is optional.
        3) destination port        <destination port>          - Eg: 80, 8080, 443.
        4) protocol                <protocol number>           - Eg: TCP=6, UDP=17.
```

# SecureXL Fast Accelerator Özelliği

## Kullanım Seçenekleri ve Örnekler

```
[Expert@PSLAB_GW01:0]#
[Expert@PSLAB_GW01:0]# fw ctl fast_accel  enable
fw fast_accel: The state has been set successfully to: enabled.
[Expert@PSLAB_GW01:0]#
```

```
[Expert@PSLAB_GW01:0]#
[Expert@PSLAB_GW01:0]# fw  ctl fast_accel add 10.255.255.80 any any any
```

Source

Destination

Destination Port

Protocol

Örnek olarak:
any veya TCP=6, UDP=17
şeklinde tanımlar set edebiliriz.

# SecureXL Fast Accelerator Özelliği

## Kullanım Seçenekleri ve Örnekler

**Kural tanımı:** **fw ctl fast_accel add «source ip» «destination ip» «D-Port» «Protocol» komutu ile sağlanır.**

```
[Expert@eFWm1:0]#
[Expert@eFWm1:0]# fw ctl fast_accel add 10.255.255.80 8.8.8.8 53 17
fw fast_accel: Please enter your full name:
admin
fw fast_accel: Rule: 10.255.255.80 8.8.8.8 53 17 has been added successfully.
[Expert@eFWm1:0]#
```

**Tanımlı kuralların listelenmesi:** **fw ctl fast_accel show_table** komutu ile sağlanır.

```
[Expert@eFWm1:0]#
[Expert@eFWm1:0]# fw ctl fast_accel show_table

------------------------------------ FIREWALL FAST ACCEL TABLE ------------------------------------
#          Source IP                Destination IP           D-Port         Protocol          Hit count
----  ------------------  ------------------  ------  --------  -----------
1)    10.255.255.80/32         8.8.8.8/32               53             17                0

[Expert@eFWm1:0]#
```

# SecureXL Fast Accelerator Özelliği

## Kullanım Seçenekleri ve Örnekler

**Tanımlı bir kuralın silinmesi:** **fw ctl fast_accel delete «source ip» «destination ip» «D-Port» «Protocol»** komutu ile sağlanır.

```
[Expert@eFWm1:0]#
[Expert@eFWm1:0]# fw ctl fast_accel delete 10.255.255.80/32 8.8.8.8/32 53 17
fw fast_accel: Please enter your full name:
admin
fw fast_accel: Rule: 10.255.255.80/32 8.8.8.8/32 53 17 has been deleted successfully.
[Expert@eFWm1:0]#
```

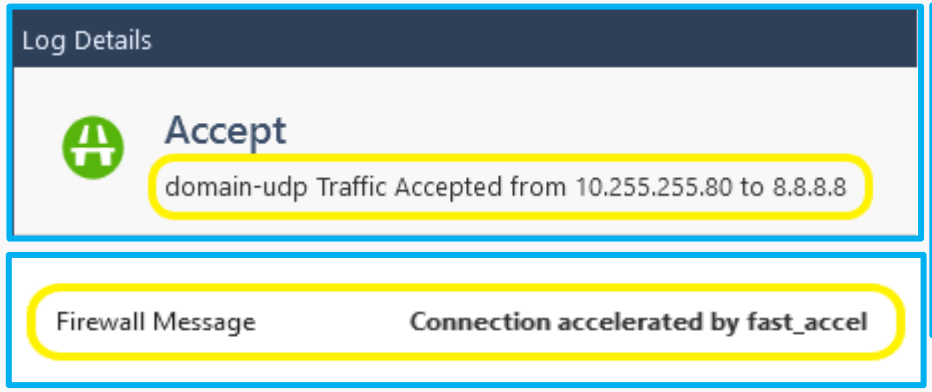
**Tanımların export edilmesi:** **fw ctl fast_accel export_conf** komutu ile sağlanır.

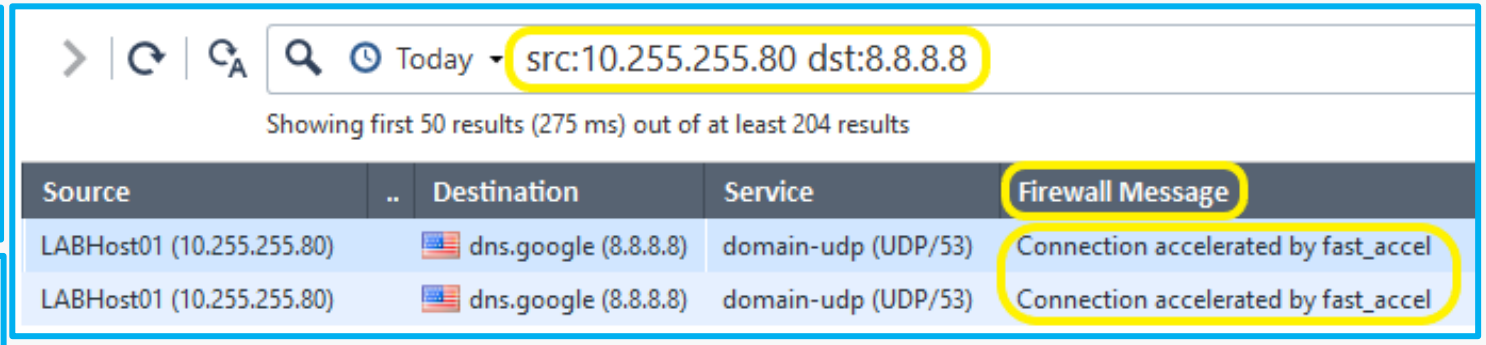
```
[Expert@eFWm1:0]#
[Expert@eFWm1:0]# fw  ctl fast_accel export_conf
fw fast_accel: The export operation has been finished successfully.

The file is found in the following path: /opt/CPsuite-R81.10/fw1/conf/fw_fast_accel_export_configuration.conf

[Expert@eFWm1:0]#
[Expert@eFWm1:0]# more /opt/CPsuite-R81.10/fw1/conf/fw_fast_accel_export_configuration.conf
fw ctl fast_accel enable
echo importExportMechanism | fw ctl fast_accel delete_all
echo importExportMechanism | fw ctl fast_accel add 10.255.255.80/32          8.8.8.8/32              53          17

[Expert@eFWm1:0]#
```

# SecureXL Fast Accelerator Özelliği

## SmartLog üzerinden monitor edilmesi

Smartlog üzerinde Log Profil tanımlarını düzenleyip **«Firewall Message»** kolonunu eklediğimizde **fast accel** kapsamındaki logarı görebiliriz.




**fwaccel conns** komutu ile SecureXL kapsamındaki bağlantıları listeleyebiliriz.
Bu komut çıktısında **fast_accel** bağlantıları ise **F etiketi** ile listelenir.

**fwaccel conns | grep 8.8.8.8**

```
10.255.255.80 64167          8.8.8.8    53 17 ..N...F.........
32/40
10.255.255.80 59002          8.8.8.8   443 17 ..N...S.........
37/40
      8.8.8.8    53   10.255.255.80 64749 17 ..N...F.L.......
23/40
```

# SecureXL Fast Accelerator Özelliği

**fast_accel** komut seti ile yapılan tüm işlemler **$FWDIR/log/fw_fast_accel.log** dosyası içerisine yazılır.

```
[Expert@PSLAB_GW01:0]#
[Expert@PSLAB_GW01:0]# more $FWDIR/log/fw_fast_accel.log
          12:33:49: admin has updated the rules table by adding the rule: 10.255.255.80 any any any.
          12:48:37: admin has updated the rules table by deleting the rule: 10.255.255.80 any any any.
          12:50:14: admin has updated the rules table by adding the rule: 10.255.255.80 8.8.8.8 53 17.
[Expert@PSLAB_GW01:0]#
```

CYBER WISE

PROFESYONELSERVİSLER

# LAB NOTLARI

**Temmuz 2022**

ps-info@cyberwise.com.tr

**Hazırlayan**

**Süleyman TÖRELİ**

**Cyberwise Profesyonel Servisler Takım Lideri**

**Certified Technical Trainer (CTT+)**