Дәріс №13: Брандмауэр ішкі саясаты

1) Iptables брандмауэрінің ішкі саясаты
2) Pfsense – NGFW брандмауэрінің ішкі саясаты
3) Palo Alto 850 брандмауэрінің ішкі саясаты

1) Iptables брандмауэрінің ішкі саясаты

```
Chain INPUT (policy DROP)
Chain FORWARD (policy DROP)
Chain OUTPUT (policy DROP)
root@gulzinat-VirtualBox:/home/gulzinat#
```

Input, output және forward ережесі бойынша желі трафигі жабық

```
Chain INPUT (policy ACCEPT)
Chain FORWARD (policy DROP)
Chain OUTPUT (policy ACCEPT)
root@gulzinat-VirtualBox:/home/gulzinat#
```

Input және output ережесі бойынша желі трафигі ашық, forward ережесі бойынша желі трафигі жабық

```
Chain INPUT (policy DROP)
target     prot opt source               destination
DROP       all  --  10.10.10.10          anywhere
DROP       all  --  10.10.10.0/24        anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
root@gulzinat-VirtualBox:/home/gulzinat#
```

10.10.10.0/24 диапазонындағы IP-адреске бұғат қою

```
┌──(root㉿gulzi)-[/home/gulzi]
└─# iptables -P INPUT DROP

┌──(root㉿gulzi)-[/home/gulzi]
└─# iptables -P FORWARD DROP

┌──(root㉿gulzi)-[/home/gulzi]
└─# iptables -P OUTPUT ACCEPT

┌──(root㉿gulzi)-[/home/gulzi]
└─# iptables -A INPUT -m state --state NEW,ESTABLISHED -j  ACCEPT

┌──(root㉿gulzi)-[/home/gulzi]
└─# iptables -L -v -n
Chain INPUT (policy DROP 39 packets, 1248 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  *      *       10.10.10.10          0.0.0.0/0           tcp dpt:22
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
   25   800 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state NEW,ESTABLISHED

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

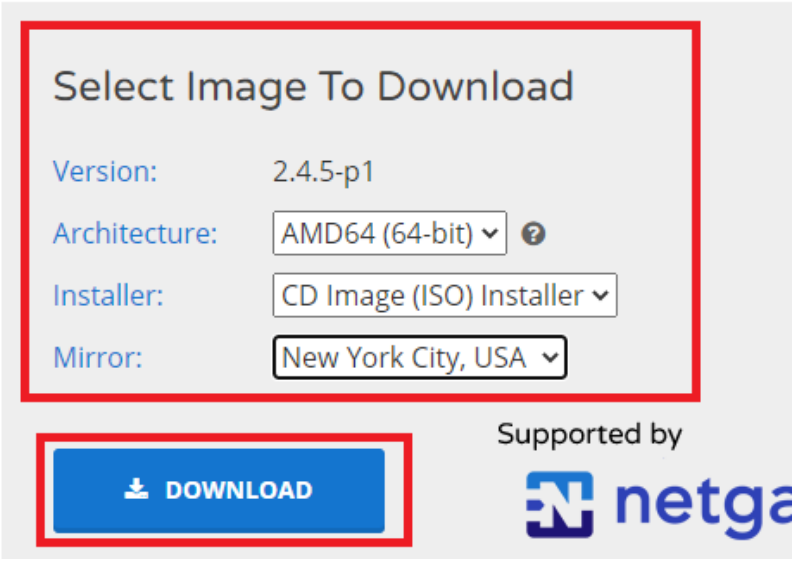
тек кіріс қосылымдарын бұғаттау

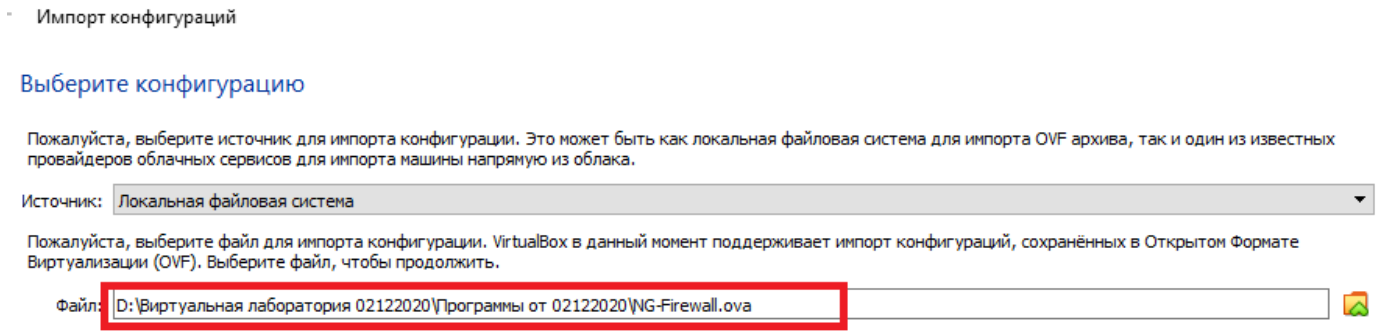
```
┌──(root💀gulzi)-[/home/gulzi]
└─# iptables -A INPUT -p tcp --dport 80 -j DROP

┌──(root💀gulzi)-[/home/gulzi]
└─# iptables -A INPUT -i eth1 -p tcp --dport 80 -j DROP

┌──(root💀gulzi)-[/home/gulzi]
└─# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
DROP       tcp  --  10.10.10.10          anywhere             tcp dpt:ssh
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     all  --  anywhere             anywhere             state NEW,ESTABLISHED
DROP       tcp  --  anywhere             anywhere             tcp dpt:http
DROP       tcp  --  anywhere             anywhere             tcp dpt:http

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

80 портынан барлық кіріс сұрауларын бұғаттау

2) Pfsense – NGFW брандмауэрінің ішкі саясаты

https://pfsense.org – арнаулы сайты





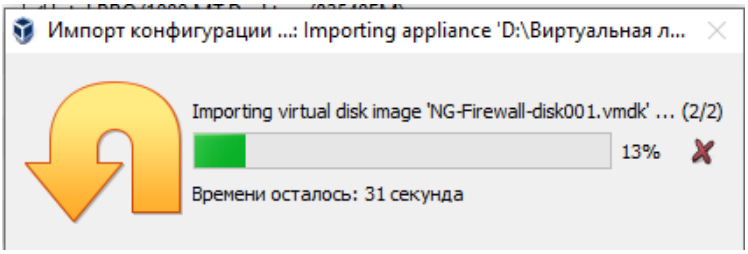
Импорт конфигураций

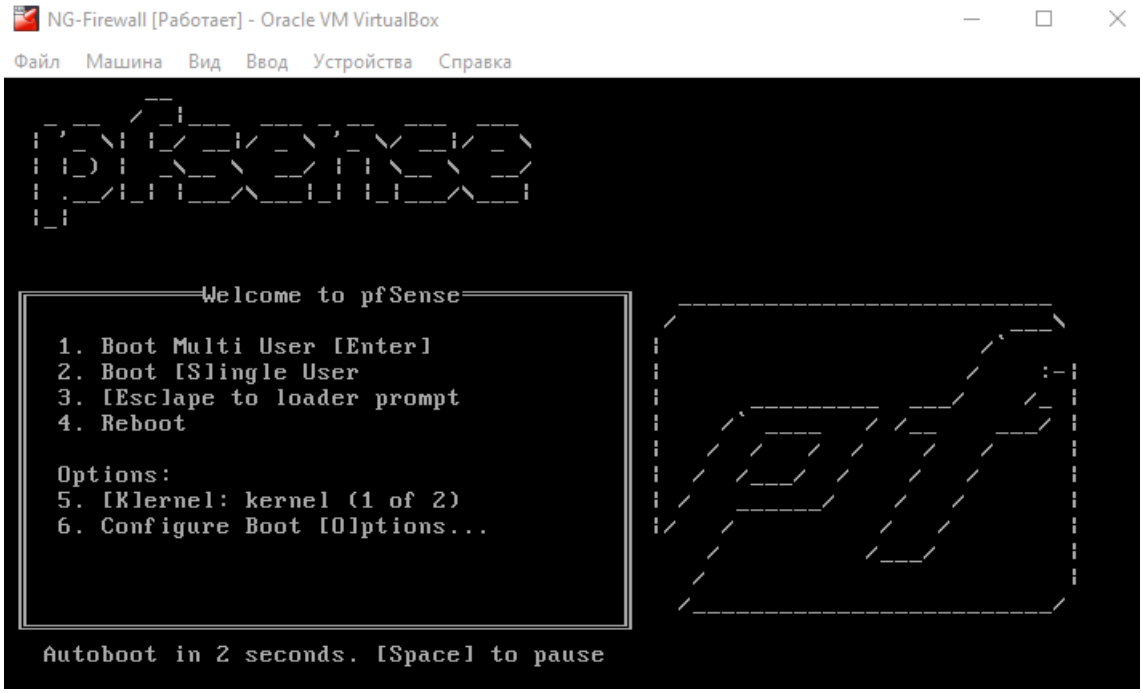
Укажите параметры импорта

Далее перечислены виртуальные машины и их устройства, описанные в импортируемой конфигурации. В
двойным щелчком мыши на выбранном элементе, либо отключить используя соответствующие галочки.

Виртуальная система 1	
Имя	NG-Firewall
Тип гостевой ОС	FreeBSD (64-bit)
Процессор	4
ОЗУ	4096 МБ
Сетевой адаптер	☑ Intel PRO/1000 MT Desktop (82540EM)
Сетевой адаптер	☑ Intel PRO/1000 MT Desktop (82540EM)
Контроллер (IDE)	PIIX4
Виртуальный образ диска	NG-Firewall-disk001.vmdk
Контроллер (IDE)	PIIX4
Базовый каталог	C:\Users\Гульзинат\VirtualBox VMs
Основная группа	/CSB-Intensive

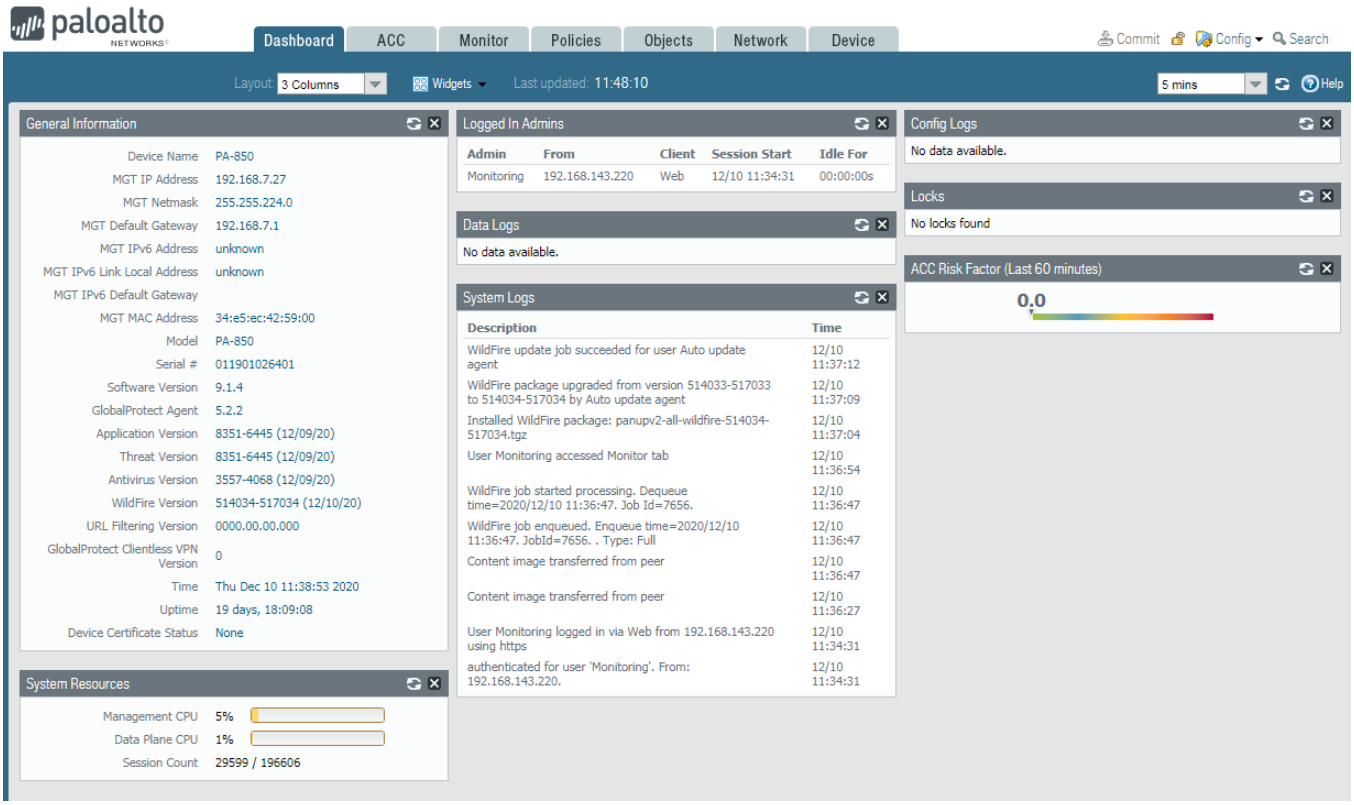
По умолчанию | Импорт | Отмена

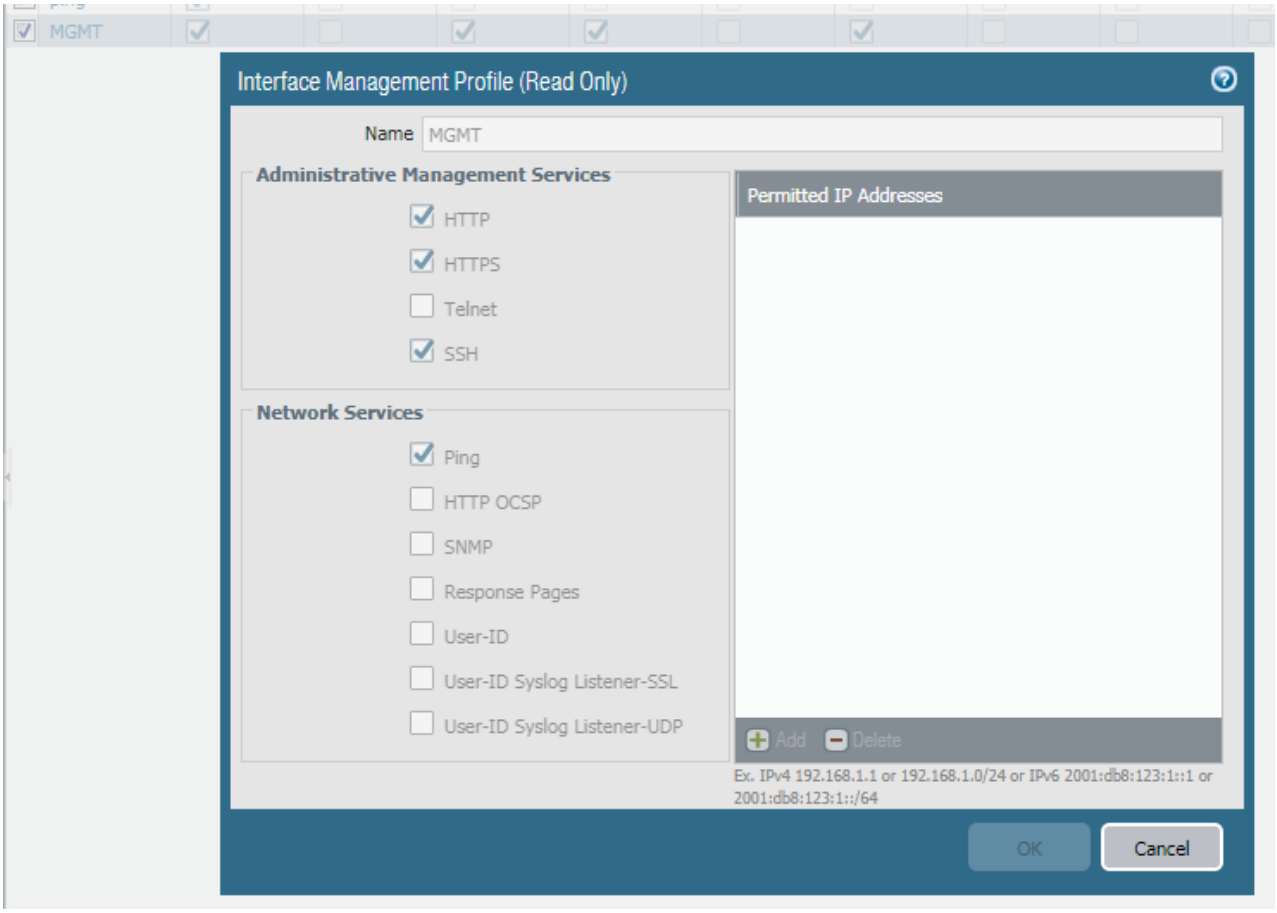


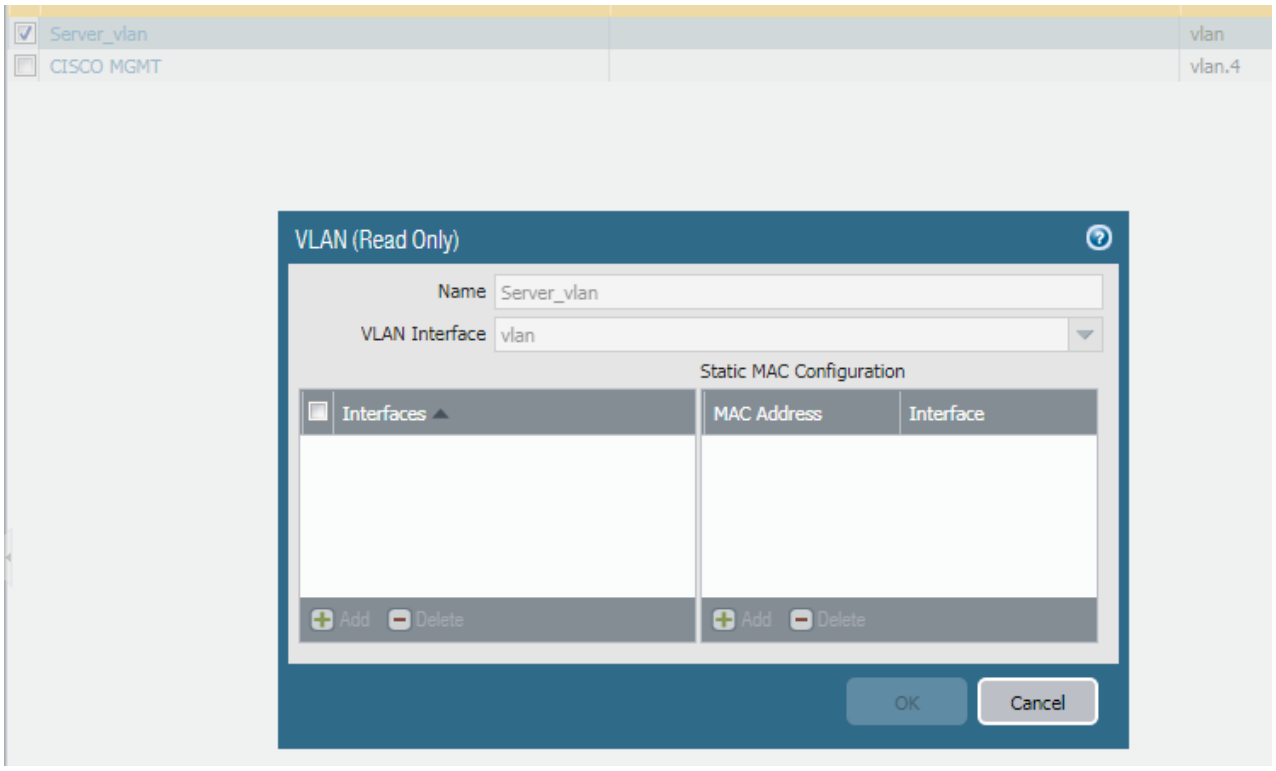


```
VirtualBox Virtual Machine - Netgate Device ID: 907defe14833396fdab3

*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on FW ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.0.16/24
 LAN (lan)       -> em1        -> v4: 192.168.125.254/24

 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:
```

3) Palo Alto 850 брандмауэрінің ішкі саясаты




MGMT
Interface Management Profile (Read Only)
Name MGMT
Administrative Management Services
HTTP
HTTPS
Telnet
SSH
Network Services
Ping
HTTP OCSP
SNMP
Response Pages
User-ID
User-ID Syslog Listener-SSL
User-ID Syslog Listener-UDP
Permitted IP Addresses
Add
Delete
Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64
OK
Cancel


Server_vlan
vlan
CISCO MGMT
vlan.4
VLAN (Read Only)
Name Server_vlan
VLAN Interface vlan
Static MAC Configuration
Interfaces
MAC Address
Interface
Add
Delete
Add
Delete
OK
Cancel

AGR_VPN_Portal		ethernet1/4	95.59.172.140/27	AGR_VPN_TLS	VPN_Users

GlobalProtect Portal Configuration (Read Only)

General
Authentication
Portal Data Collection
Agent
Clientless VPN
Satellite

Name: AGR_VPN_Portal

Network Settings

Interface: ethernet1/4
IP Address Type: IPv4 Only
IPv4 Address: 95.59.172.140/27

Appearance

Portal Login Page: factory-default
Portal Landing Page: factory-default
App Help Page: None

OK Cancel

Ethernet | VLAN | Loopback | Tunnel | SD-WAN

15 items

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	SD-W... Profile
ethernet1/1	Layer3	MGMT		192.168.4.1/24	default	Untagged	none	MGMT	
ethernet1/2	Layer3	ping		95.59.161.162/28	default	Untagged	none	Wi-Fi_Internet_Outside	
ethernet1/3	Layer3	ping		none	none	Untagged	none	none	
ethernet1/4	Layer3	ping		95.59.172.140/27	default	Untagged	none	internet	
ethernet1/5	Layer3	ping		none	none	Untagged	none	none	
ethernet1/6	Layer3			none	default	Untagged	none	none	
ethernet1/6.101	Layer3	MGMT		192.168.96.1/19	default	101	none	Local_Users	
ethernet1/6.102	Layer3	ping		192.168.128.1/19	default	102	none	Local_Users	
ethernet1/6.200	Layer3	ping		192.168.200.200/24	default	200	none	Accounts	
ethernet1/7	Layer3	MGMT		192.168.7.1/24	default	Untagged	none	Servers	
ethernet1/8	Layer3	ping		172.17.1.2/16	default	Untagged	none	WiFi	
ethernet1/9	Layer3			none	none	Untagged	none	none	
ethernet1/10	Layer3			none	none	Untagged	none	none	
ethernet1/11	Layer3			none	none	Untagged	none	none	
ethernet1/12	Layer3			none	none	Untagged	none	none	

Ethernet Interface (Read Only)

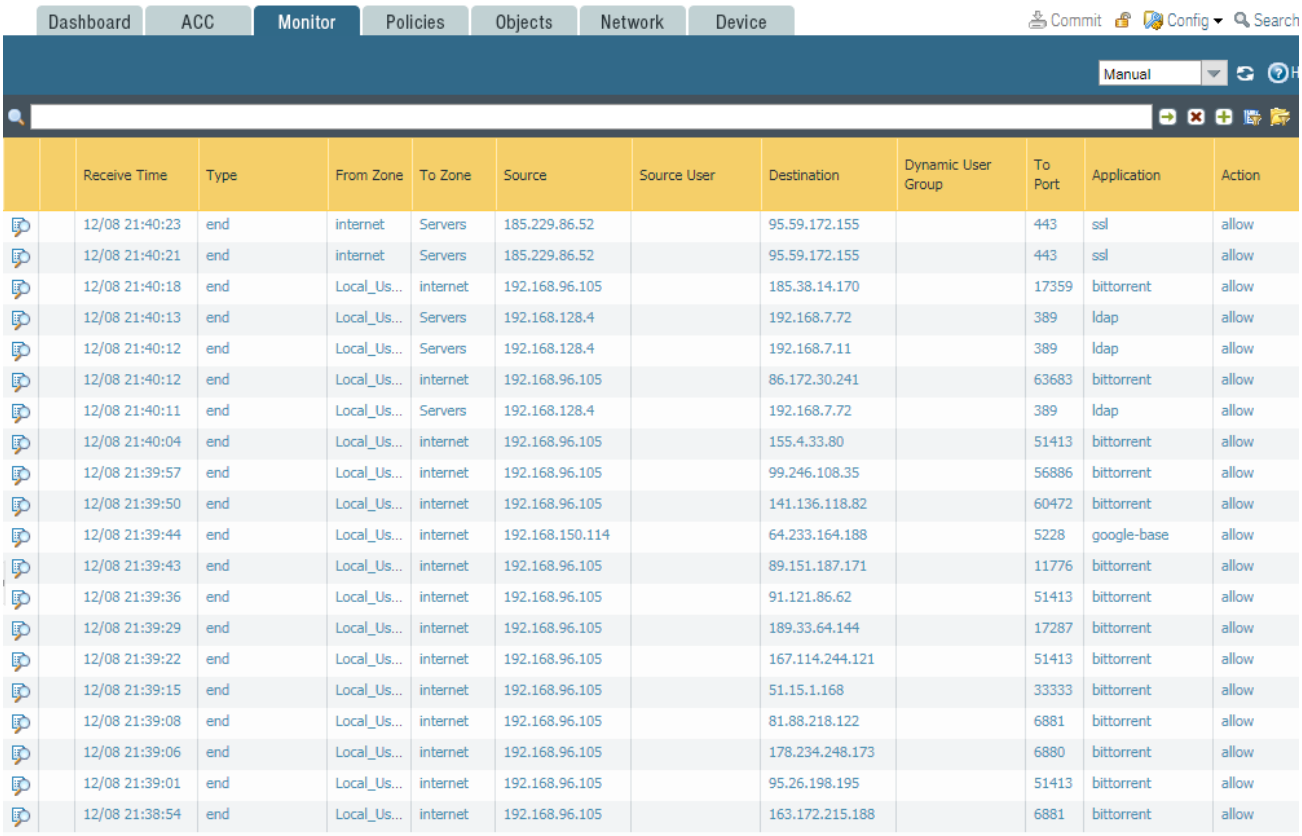
Interface Name: ethernet1/1
Comment: CISCO
Interface Type: Layer3
Netflow Profile: None

Config | IPv4 | IPv6 | SD-WAN | Advanced

Assign Interface To

Virtual Router: default
Security Zone: MGMT

OK Cancel



		Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	Dynamic User Group	To Port	Application	Action
		12/08 21:40:23	end	internet	Servers	185.229.86.52		95.59.172.155		443	ssl	allow
		12/08 21:40:21	end	internet	Servers	185.229.86.52		95.59.172.155		443	ssl	allow
		12/08 21:40:18	end	Local_Us...	internet	192.168.96.105		185.38.14.170		17359	bittorrent	allow
		12/08 21:40:13	end	Local_Us...	Servers	192.168.128.4		192.168.7.72		389	ldap	allow
		12/08 21:40:12	end	Local_Us...	Servers	192.168.128.4		192.168.7.11		389	ldap	allow
		12/08 21:40:12	end	Local_Us...	internet	192.168.96.105		86.172.30.241		63683	bittorrent	allow
		12/08 21:40:11	end	Local_Us...	Servers	192.168.128.4		192.168.7.72		389	ldap	allow
		12/08 21:40:04	end	Local_Us...	internet	192.168.96.105		155.4.33.80		51413	bittorrent	allow
		12/08 21:39:57	end	Local_Us...	internet	192.168.96.105		99.246.108.35		56886	bittorrent	allow
		12/08 21:39:50	end	Local_Us...	internet	192.168.96.105		141.136.118.82		60472	bittorrent	allow
		12/08 21:39:44	end	Local_Us...	internet	192.168.150.114		64.233.164.188		5228	google-base	allow
		12/08 21:39:43	end	Local_Us...	internet	192.168.96.105		89.151.187.171		11776	bittorrent	allow
		12/08 21:39:36	end	Local_Us...	internet	192.168.96.105		91.121.86.62		51413	bittorrent	allow
		12/08 21:39:29	end	Local_Us...	internet	192.168.96.105		189.33.64.144		17287	bittorrent	allow
		12/08 21:39:22	end	Local_Us...	internet	192.168.96.105		167.114.244.121		51413	bittorrent	allow
		12/08 21:39:15	end	Local_Us...	internet	192.168.96.105		51.15.1.168		33333	bittorrent	allow
		12/08 21:39:08	end	Local_Us...	internet	192.168.96.105		81.88.218.122		6881	bittorrent	allow
		12/08 21:39:06	end	Local_Us...	internet	192.168.96.105		178.234.248.173		6880	bittorrent	allow
		12/08 21:39:01	end	Local_Us...	internet	192.168.96.105		95.26.198.195		51413	bittorrent	allow
		12/08 21:38:54	end	Local_Us...	internet	192.168.96.105		163.172.215.188		6881	bittorrent	allow

Policy Based

	Name	Tags	Source			Destination	Application	Service	Action	Egres
			Zone/Interface	Address	User	Address				
1	WiFi_domain_Access...	none	WiFi	any	any	192.168.7.54 192.168.7.61 192.168.7.62 192.168.7.65 192.168.7.66 192.168.7.67 192.168.7.68 more...	any	any	no-pbf	none
2	WiFi_to_local	none	WiFi	any	any	Main_Building	any	any	no-pbf	none
3	wifi_routing	none	WiFi	any	any	any	any	any	forward	ethern
4	Local_to_bbb3	none	Local_Users	any	any	95.59.161.170	any	any	forward	ethern