

Główne założenia:

- IPSec LAN-LAN z routingiem pomiędzy podsieciami Vigor2920(192.168.1.0/24) a Vigor2960 (192.168.0.0/24)
- tylko PC 192.168.1.10 ma dostęp do Serwera 192.168.0.10 – pozostałe urządzenia z 192.168.1.0/24 nie mają dostępu do 192.168.0.0/24

W przykładzie pominięto konfigurację VPN.

VPN and Remote Access >> Connection Management >> Connection Management

Connection Management History

Dial-Out tool
 IPsec PPTP Profiles: [dropdown] [Connect] [Refresh]

VPN Connection Status

VPN	Type	Interface	Remote IP	Virtual Network	Up Time	RX(Packets)	TX(Packets)	Operation	
1	ipsec_in	IPsec/AES_HMA...	wan1	99.99.99.11	192.168.1.0/24	00:00:29	1117	2039	[stop] [refresh]

Przejdź do zakładki **Object Settings>>IP Object**. Stwórz odpowiednie profile adresów IP.

Objects Setting >> IP Object

IP Object

Add Edit Delete Refresh Profile Number Limit : 200

Profile	Address Type	Start IP Address	End IP Address	Subnet Mask
1 subnet_local	Subnet	192.168.0.0		255.255.255.0
2 server_local	Single	192.168.0.10		
3 subnet_remote	Subnet	192.168.1.0		255.255.255.0
4 PC_remote	Single	192.168.1.10		

IP Object

Profile : subnet_local

Address Type : Subnet

Start IP Address : 192 . 168 . 0 . 0

Subnet Mask : 255.255.255.0/24

IP Object

Profile : server_local

Address Type : Single

Start IP Address : 192 . 168 . 0 . 10

IP Object

Profile : subnet_remote

Address Type : Subnet

Start IP Address : 192 . 168 . 1 . 0

Subnet Mask : 255.255.255.0/24

IP Object

Profile : PC_remote

Address Type : Single

Start IP Address : 192 . 168 . 1 . 10

Przejdź do zakładki **Firewall>>Filter Setup>>IP Filter**. Stwórz odpowiednią grupę oraz reguły wybierając wcześniej stworzone profile obiektów.

Firewall >> Filter Setup >> IP Filter

IP Filter IPv6 Filter Application Filter URL/Web Category Filter QQ Filter Default Policy

Add Edit Delete Refresh Move Up Move Down Profile Number Limit : 12

Group	Enable	Comment
vpn_control	true	

Add Edit Delete Refresh Rename Move Up Move Down Profile Number Limit

Rule	Enable	Action	Next Group For F...	Syslog	Source LDAP Gro...	General Firewall ...	Source Firewall T...	Destination Firew...
PC_remote_pass	true	pass		Disable			PC_remote	server_local
subnet_remote_block	true	block		Disable			subnet_remote	subnet_local

Rule - X

Profile : PC_remote_pass

Enable

Block Action : Pass

Next Group :

SysLog : Enable Disable

Input Interface : Any

Output Interface : Any

While no target has been specified, firewall rules are applied to Any object

Firewall Objects

- Time Schedule
 - ▶ Time Object
 - ▶ Time Group
- Service Protocol
 - ▶ Service Type Object
 - ▶ Service Type Group
- Incoming Country Filter
 - ▶ Source Country Object (At most accept 15 countries)
- Out-going Country Filter
 - ▶ Destination Country Object (At most accept 15 countries)
- Source IP
 - ▶ Source IP Object

<input type="checkbox"/>	Profile	Address Type	Start IP Address	End IP Address	Subnet Mask	Edit
<input type="checkbox"/>	subnet_local	Subnet	192.168.0.0		255.255.255.0	✕
<input type="checkbox"/>	server_local	Single	192.168.0.10			✕
<input type="checkbox"/>	subnet_remote	Subnet	192.168.1.0		255.255.255.0	✕
<input checked="" type="checkbox"/>	PC_remote	Single	192.168.1.10			✕
 - ▶ Source IP Group
 - ▶ Source User Profile
 - ▶ Source User Group
 - ▶ Source LDAP Group- Destination IP
 - ▶ Destination IP Object

<input type="checkbox"/>	Profile	Address Type	Start IP Address	End IP Address	Subnet Mask	Edit
<input type="checkbox"/>	subnet_local	Subnet	192.168.0.0		255.255.255.0	✕
<input checked="" type="checkbox"/>	server_local	Single	192.168.0.10			✕
<input type="checkbox"/>	subnet_remote	Subnet	192.168.1.0		255.255.255.0	✕
<input type="checkbox"/>	PC_remote	Single	192.168.1.10			✕
 - ▶ Destination IP Group
 - ▶ Destination DNS Object
 - ▶ Destination User Profile
 - ▶ Destination User Group
 - ▶ Destination LDAP Group

Rule [-] [X]

Profile : subnet_remote_block

Enable

Block Action : Block [v]

Next Group : [v]

SysLog : Enable Disable

Input Interface : Any [v]

Output Interface : Any [v]

While no target has been specified, firewall rules are applied to Any object

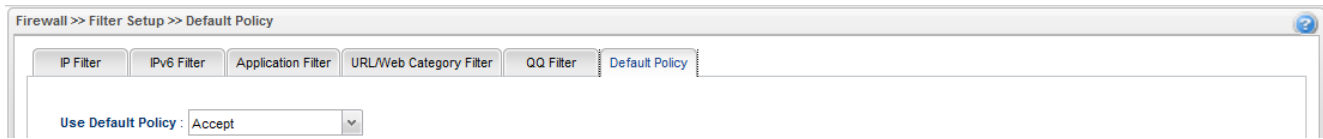
Firewall Objects

- Time Schedule
 - ▶ Time Object
 - ▶ Time Group
- Service Protocol
 - ▶ Service Type Object
 - ▶ Service Type Group
- Incoming Country Filter
 - ▶ Source Country Object (At most accept 15 countries)
- Out-going Country Filter
 - ▶ Destination Country Object (At most accept 15 countries)
- Source IP
 - ▶ Source IP Object

<input type="checkbox"/>	Profile	Address Type	Start IP Address	End IP Address	Subnet Mask	Edit
<input type="checkbox"/>	subnet_local	Subnet	192.168.0.0		255.255.255.0	
<input type="checkbox"/>	server_local	Single	192.168.0.10			
<input checked="" type="checkbox"/>	subnet_remote	Subnet	192.168.1.0		255.255.255.0	
<input type="checkbox"/>	PC_remote	Single	192.168.1.10			
 - ▶ Source IP Group
 - ▶ Source User Profile
 - ▶ Source User Group
 - ▶ Source LDAP Group
 - Destination IP
 - ▶ Destination IP Object

<input type="checkbox"/>	Profile	Address Type	Start IP Address	End IP Address	Subnet Mask	Edit
<input checked="" type="checkbox"/>	subnet_local	Subnet	192.168.0.0		255.255.255.0	
<input type="checkbox"/>	server_local	Single	192.168.0.10			
<input type="checkbox"/>	subnet_remote	Subnet	192.168.1.0		255.255.255.0	
<input type="checkbox"/>	PC_remote	Single	192.168.1.10			
 - ▶ Destination IP Group
 - ▶ Destination DNS Object
 - ▶ Destination User Profile
 - ▶ Destination User Group
 - ▶ Destination LDAP Group

Przejdź do zakładki **Firewall>>Filter Setup>>Default Policy**. Domyślnie router przepuszcza ruch do Internetu, który nie spełnia kryteriów Filtru IP, Filtru Aplikacji, Filtru URL/Kategorii Web.



Krzysztof Skowina
Specjalista ds. rozwiązań sieciowych
BRINET Sp. z o.o.
k.skowina@brinet.pl