NETGEAR-FVX538

Relation

Fabrizio Celli;Fabio Papacchini;Andrea Gozzi

-2008-

Abstract

Summary 2

Chapter 1: Introduction 4

Chapter 2: LAN 6

2.1 LAN Configuration 6

2.1.1 First experiment: DoS attack 6

2.1.2 Second experiment: MAC filter 7

2.1.3 Third experiment: MitM attack 7

2.1.4 Fourth experiment: switch infinitive loop 8

Chapter 3: WAN 9

3.1 WAN Configuration 9

3.1.1 Hping attack 11

3.1.2 Port Scan 11

Chapter 4: VPN 12

4.1 VPN Configuration 12

4.1.1 Sniffing VPN startup 14

Summary

Property	Netgear FVX538	Page
Firewall?	yes, stateful	
Router?	broadband router	
Ids/Ips/Content Filtering	only content filtering (spi)	
ISO-OSI level of work	transport level (lv4)	
Antivirus?	no	
Anti-Spyware?	no	
Wireless?	no	
Dmz hardware port?	yes	9
Dmz policy configuration?	yes	9
memory DRAM	32 MB	
CPU speed	533 Mhz	
Lan to Wan throughput	80 Mbps	
Real throughput	7 MByte/s => 56 Mbps	
VPN IPSec throughput	1.8 MByte/s => 14.4 Mbps	
Load balancing	yes	
Failover	yes	
Classical routing mode	yes	
Static IP assignment	yes	
Remote logging	syslog	
DHCP client/server	yes	
concurrent sessions	10000	
dedicated VPN tunnels	200	
VPN protocols supported	IPSec, ESP	
IPSec encryption	256-bit AES, 168-bit 3DES	
polices	yes	
warranty	forever	4
firmware update	yes, every month. This isn't an IDS, so it does not need daily updates.	4
forum	yes, http://forum1.netgear.com/index.php. To write in this forum, you need to register your product	4
business policy	NETGEAR’s policy aims to equip all models with the same security features. What changes is the computing power and the data processing ability.	4
internal spanning tree	no, in fact a simple loop on the switch causes a crash	8

external port scan	firewall logs external port scans but it doesn't block them. We obtained a list of all open ports on WAN interface	
Tor usage block or log	no	
Vlan	not available	
Sniffing VPN password exchange	we sniffed the conversation and also the password exchange, but all the conversation is ciphered, so an attacker can only try the “cipher-text only attack”	4.112
Experiments	- Dos attack from LAN - MitM from LAN - Switch infinitive loop - MAC filtering - DMZ policies - TOR - Dos attack from WAN - Port Scan from LAN and WAN - VPN configuration - VPN traffic measurement - VPN sniffing startup - VPN sniffing communication	

Chapter 1: Introduction

ProSafe Dual WAN VPN Firewall FVX538 offers a complete security solution for small and medium-sized companies. This stateful packet inspection (SPI) firewall is equipped with support for up to 200 security associations (VPN tunnels). The FVX538 can serve as a DHCP server, supports Simple Network Management Protocol (SNMP), Quality of Service (QoS) and has a powerful SPI firewall to protect PCs against intruders and most common Internet attacks.

Featuring eight 10/100 Mbps LAN ports, one Gigabit LAN port and two 10/100 WAN ports, the VPN Firewall FVX538 lets multiple computers share two Internet connections. The dual WAN ports let you connect a second Internet line as a backup to insure that you're never disconnected. One LAN port can be dedicated as a hardware DMZ port for safely providing services to the Internet without compromising security on your LAN.

Specification

As mentioned, VPN Firewall FVX538 is equipped with eight 10/100 Mbps LAN ports, a Gigabit LAN port and a designated port to be dedicated to configure a DMZ.

In addition there are two WAN ports carrying a load balancing automatically.

Finally, it has a serial port, to support a CLI (command line interface).

Looking at the security features, we can state that VPN Firewall FVX538:

- is a SPI firewall: it offers Stateful Packet Inspection to prevent notorious denial of service attacks (DoS). This service is supported by logging activities, that allows to report the alarms, eventually by e-mail. The firewall also offers the Web URL keyword filtering, to prevent the so-called "reassembly attack", and the port/service blocking.
- supports VPN feature with the opportunity to set up 200 dedicated VPN tunnels
- supports the 'perfect forward secrecy'
- implements policies for IP security as the algorithms IPsec-based 56-bit (DES), 168-bit (3DES), or 256-bit (AES)
- supports one-to-one and many-to-many Multi-Network Address Translation, classical routing and it has no restriction regarding the use of doors by the users
- supports different modes of Ip addresses assignment such as: static assignment, DHCP server on the internal LAN, DHCP client on the WAN, PPPoE client support.

Warranty (http://www.netgear.com/warranty)

Since May 1, 2007 NETGEAR is offering a life time warranty on its Prosafe products. It means that when a client buys a Prosafe product, NETGEAR offers its willingness to change the product in case of fault, requiring only an original proof of purchase.

In this way NETGEAR demonstrate its certainty about the reliability of its products.

Firmware Update and Product Registration

Because Prosafe VPN Firewall FVX538 is not an IDS or an IPS instrument, **there isn't the need to frequently update the database of attacks.**

So NETGEAR offers the opportunity to update only the product's firmware, with variable frequency (sometimes a month, sometimes two).

These updates can be downloaded from the site without the need of the registration of the product, that is not necessary to obtain this kind of benefits: it allows only phone support and facilities on the other NETGEAR products on the market.

Support Page (http://kbserver.netgear.com/products/FVX538v2.asp)

For each NETGEAR product exists a support page that can be useful to the users for various reasons. It contains the links to the new released firmware versions, in which are described the bugs fixed by each version and those known but not yet resolved, and there is the possibility to download them.

There are also different examples of configuration for the firewall, for example to configure a VPN, to use the Multi-NAT feature or the port forwarding, so everything that a not expert user may need, and it is described also the procedure to execute in case of updating firmware failure.

There are also available all the product's documents, like the user manual, the installation guide, etc.

Forum e Customer Service

Finally, an online Customer Care and a discussion forum are available.

By the Customer Care (http://kbserver.netgear.com/kb_web_files/customer_service/main.htm) it is possible to request information about some product or some feature to competent staff.

The forum (http://forum1.netgear.com/index.php) allows users to exchange information and opinions about products, and works as a community to allow anyone to learn new things by public discussions.

Products Comparison

It's easy to guess that NETGEAR's policy aim to equip its four models of Wired VPN Firewalls with the same security features. What changes is the computing power and the data processing ability.

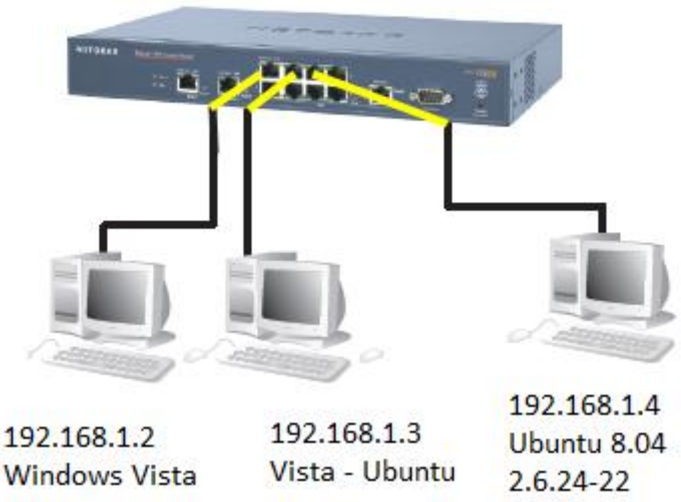
We can see that all the four models provide SPI functionality to prevent DoS attacks, NAT/PAT, QoS, DMZ, VPN, Ipsec, Logging (SYSLOG), but for example VPN Firewall FVS318 offers the possibility to configure eight VPN dedicated tunnels, while the FVX538 even 200.

However, the differences are especially in terms of performance: we can see a strong difference in throughput, memory, processor, etc…

Chapter 2: LAN

2.1 LAN Configuration

As we have said in the introduction, this firewall considers a LAN as trusted. So we tried to realize some attacks to verify this assertion. We configured the LAN as follow:



IP addresses has been configured as static IPs.

2.1.1 First experiment: DoS attack

192.168.1.4 started to send a continuous flow of large packets by using hping3 instrument with destination IP address equal to the IP address of the Firewall (192.168.1.1). In a short time, Firewall's memory has been saturated and it stopped working: the DoS attack was successful.

In particular, we tried a Syn Flood attack after having blocked this kind of attack inside the firewall, using default rules:

```
hping3 -S -i u1 192.168.1.1
```

where parameters have the following meaning:

- -S: sends TCP packets having SYN flag set
- -i u1: sends a packet every millisecond

After a few seconds, we were no more able to access the firewall by browser (192.168.1.1) neither to connect our machines to Internet.

We have therefore tried to send UDP packets, activating inside the firewall the limit of maximum UDP connections. The command is:

```
hping3 -2 -i u1 192.168.1.1
```

where −2 option is used to send UDP packets.
As we expected the firewall has not even prevented this new attack filling again its memory in a very short time.
Another attempt was made by sending ICMP packets (-1 option) with results similar to the previous.

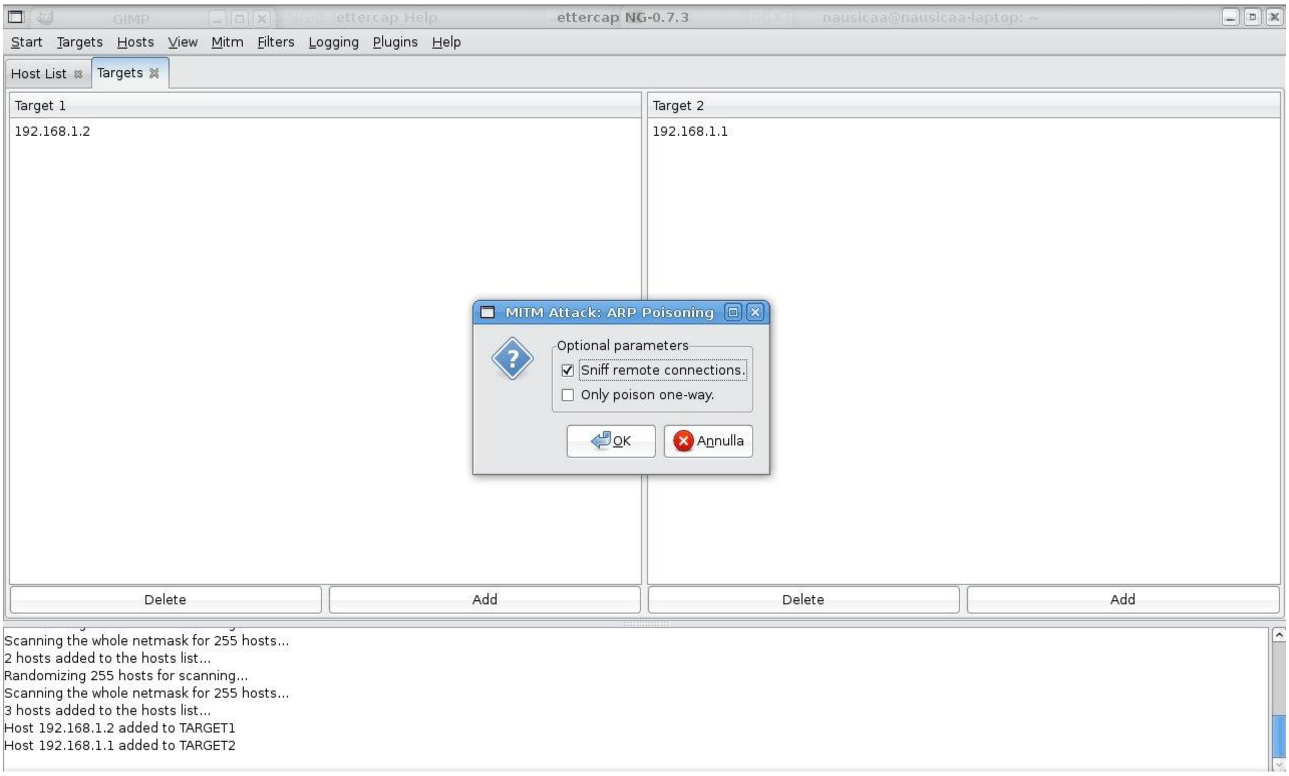
CONCLUSION: this firewall considers LAN as trusted (and it was foreseeable because it is only a switch), so it blocks only attacks from/to the WAN. In this way, a malevolent user inside the LAN can execute a DoS attack to every other users of the LAN, realize MitM attack and sniffing.

2.1.2 Second experiment: MAC filter

We tried to avoid these attacks using Firewall MAC filter: this is a dirty solution because it limits the users that can connect to the LAN by setting statically the IP-MAC correspondence. In this case, we blocked all attacks because 192.168.1.4 was no more able to connect to the LAN.

2.1.3 Third experiment: MitM attack

To say the truth, 192.168.1.4 is a very malevolent user, so he decided to use ETTERCAP NG-0.7.3 to realize Man in the Middle attack.
192.168.1.4 scans all the hosts of LAN and decides to attack 192.168.1.2: he puts himself between 192.168.1.2 and the firewall, so he starts passive MitM. In this way he was able to read all packets between the firewall and the target and to decide to block some of them: so starting Apache 2.2 on 192.168.1.2, the attacker can realize a simple DoS by blocking the forwarding of the answer of 192.168.1.2.



Target 1	Target 2
192.168.1.2	192.168.1.1

Optional parameters

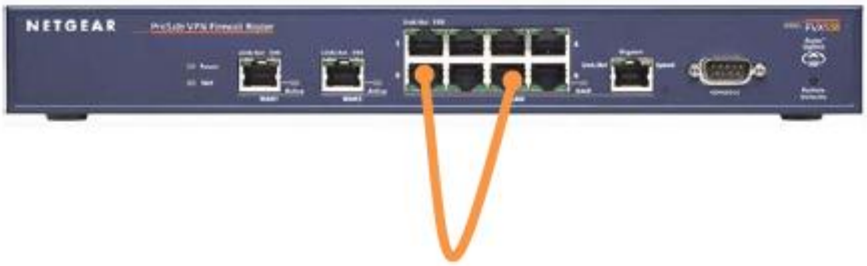
☑ Sniff remote connections.

□ Only poison one-way.

```
Scanning the whole netmask for 255 hosts...
2 hosts added to the hosts list...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
Host 192.168.1.2 added to TARGET1
Host 192.168.1.1 added to TARGET2
```

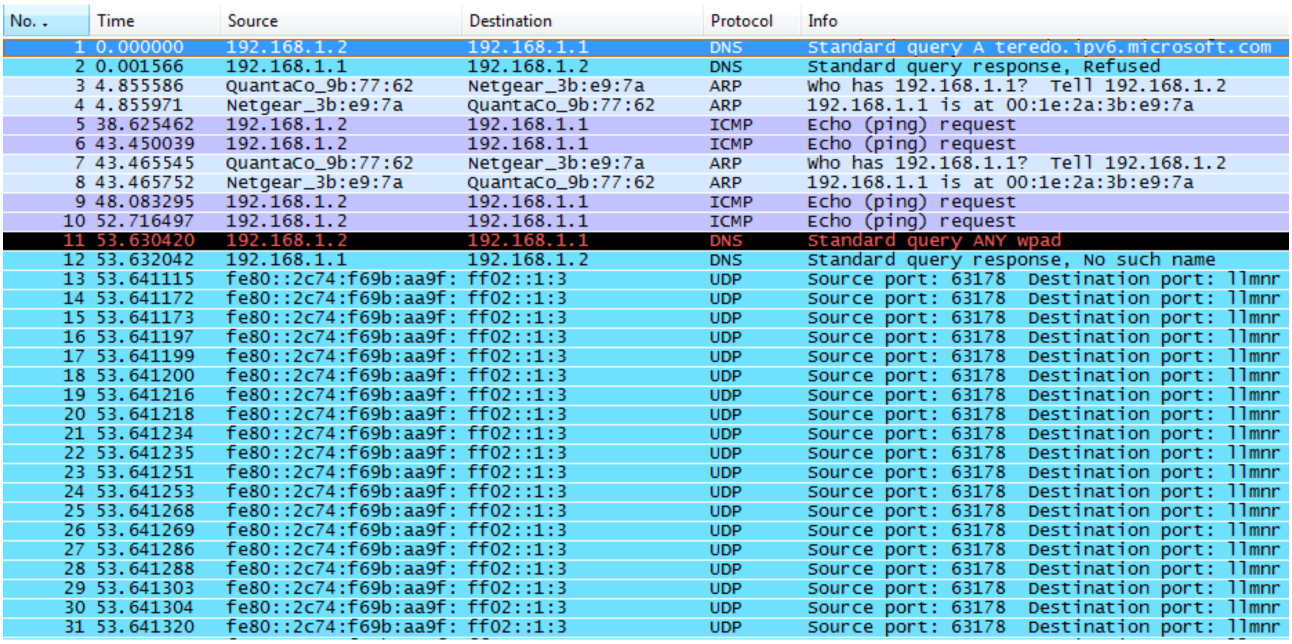
2.1.4 Fourth experiment: switch infinitive loop

We realized the following experiment to saturate the firewall. We connected a single Ethernet cable to the switch in order to create a loop:



Then we connected also a PC to the switch and we execute a "ping" on the firewall interface. A great quantity of traffic started to run inside the loop so that the firewall immediately saturated and it was no more possible to accede to the configuration page.

This is a screenshot of Wireshark:

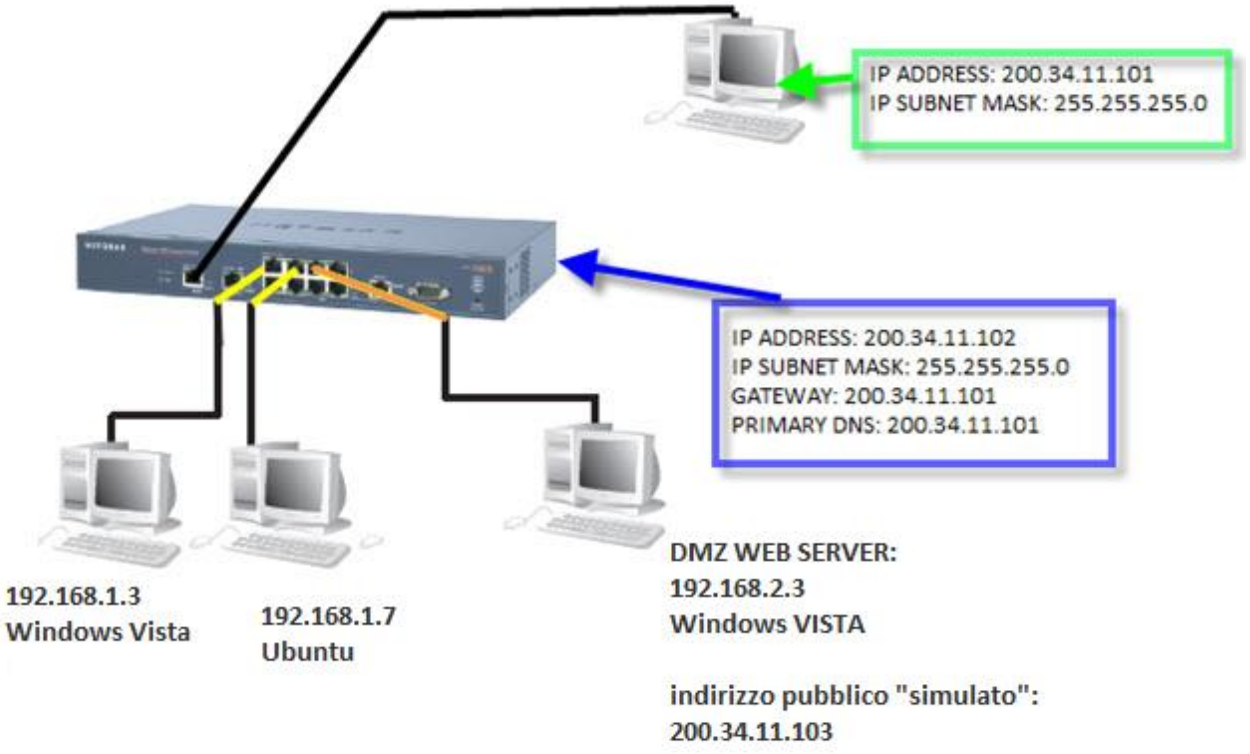


No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.2	192.168.1.1	DNS	Standard query A teredo.ipv6.microsoft.com
2	0.001566	192.168.1.1	192.168.1.2	DNS	Standard query response, Refused
3	4.855586	QuantaCo_9b:77:62	Netgear_3b:e9:7a	ARP	Who has 192.168.1.1? Tell 192.168.1.2
4	4.855971	Netgear_3b:e9:7a	QuantaCo_9b:77:62	ARP	192.168.1.1 is at 00:1e:2a:3b:e9:7a
5	38.625462	192.168.1.2	192.168.1.1	ICMP	Echo (ping) request
6	43.450039	192.168.1.2	192.168.1.1	ICMP	Echo (ping) request
7	43.465545	QuantaCo_9b:77:62	Netgear_3b:e9:7a	ARP	Who has 192.168.1.1? Tell 192.168.1.2
8	43.465752	Netgear_3b:e9:7a	QuantaCo_9b:77:62	ARP	192.168.1.1 is at 00:1e:2a:3b:e9:7a
9	48.083295	192.168.1.2	192.168.1.1	ICMP	Echo (ping) request
10	52.716497	192.168.1.2	192.168.1.1	ICMP	Echo (ping) request
11	53.630420	192.168.1.2	192.168.1.1	DNS	Standard query ANY wpad
12	53.632042	192.168.1.1	192.168.1.2	DNS	Standard query response, No such name
13	53.641115	fe80::2c74:f69b:aa9f:	ff02::1:3	UDP	Source port: 63178 Destination port: llmnr
14	53.641172	fe80::2c74:f69b:aa9f:	ff02::1:3	UDP	Source port: 63178 Destination port: llmnr
15	53.641173	fe80::2c74:f69b:aa9f:	ff02::1:3	UDP	Source port: 63178 Destination port: llmnr
16	53.641197	fe80::2c74:f69b:aa9f:	ff02::1:3	UDP	Source port: 63178 Destination port: llmnr
17	53.641199	fe80::2c74:f69b:aa9f:	ff02::1:3	UDP	Source port: 63178 Destination port: llmnr
18	53.641200	fe80::2c74:f69b:aa9f:	ff02::1:3	UDP	Source port: 63178 Destination port: llmnr
19	53.641216	fe80::2c74:f69b:aa9f:	ff02::1:3	UDP	Source port: 63178 Destination port: llmnr
20	53.641218	fe80::2c74:f69b:aa9f:	ff02::1:3	UDP	Source port: 63178 Destination port: llmnr
21	53.641234	fe80::2c74:f69b:aa9f:	ff02::1:3	UDP	Source port: 63178 Destination port: llmnr
22	53.641235	fe80::2c74:f69b:aa9f:	ff02::1:3	UDP	Source port: 63178 Destination port: llmnr
23	53.641251	fe80::2c74:f69b:aa9f:	ff02::1:3	UDP	Source port: 63178 Destination port: llmnr
24	53.641253	fe80::2c74:f69b:aa9f:	ff02::1:3	UDP	Source port: 63178 Destination port: llmnr
25	53.641268	fe80::2c74:f69b:aa9f:	ff02::1:3	UDP	Source port: 63178 Destination port: llmnr
26	53.641269	fe80::2c74:f69b:aa9f:	ff02::1:3	UDP	Source port: 63178 Destination port: llmnr
27	53.641286	fe80::2c74:f69b:aa9f:	ff02::1:3	UDP	Source port: 63178 Destination port: llmnr
28	53.641288	fe80::2c74:f69b:aa9f:	ff02::1:3	UDP	Source port: 63178 Destination port: llmnr
29	53.641303	fe80::2c74:f69b:aa9f:	ff02::1:3	UDP	Source port: 63178 Destination port: llmnr
30	53.641304	fe80::2c74:f69b:aa9f:	ff02::1:3	UDP	Source port: 63178 Destination port: llmnr
31	53.641320	fe80::2c74:f69b:aa9f:	ff02::1:3	UDP	Source port: 63178 Destination port: llmnr

Chapter 3: WAN

3.1 WAN Configuration

We configured a PC on Wan1 port and we put a web server on DMZ port.



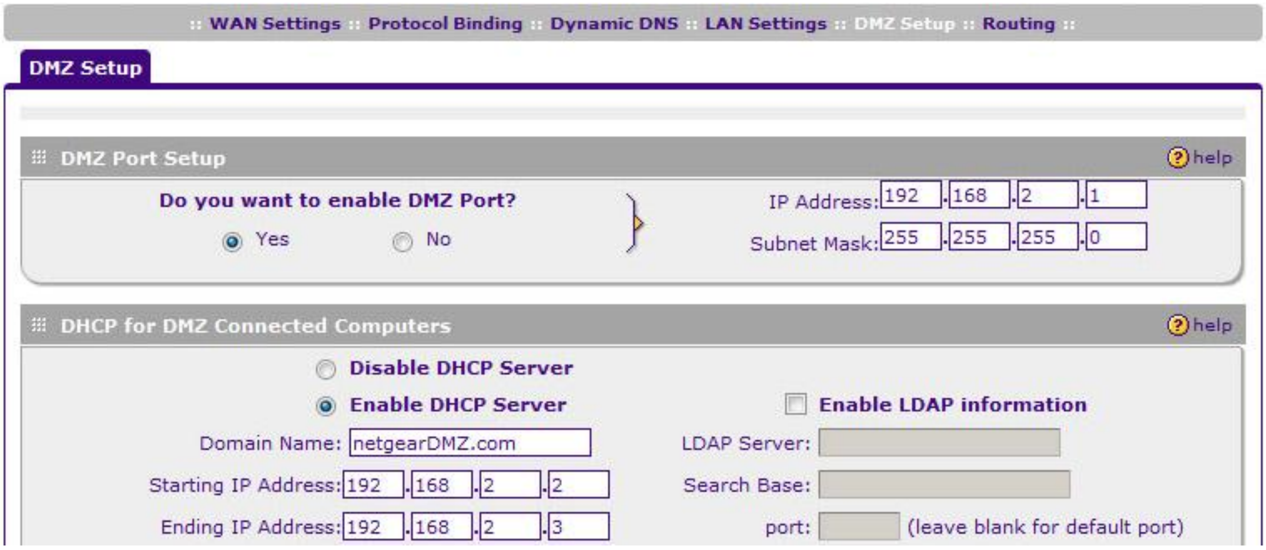
IP ADDRESS: 200.34.11.101
IP SUBNET MASK: 255.255.255.0
IP ADDRESS: 200.34.11.102
IP SUBNET MASK: 255.255.255.0
GATEWAY: 200.34.11.101
PRIMARY DNS: 200.34.11.101
192.168.1.3
Windows Vista
192.168.1.7
Ubuntu
DMZ WEB SERVER:
192.168.2.3
Windows VISTA
indirizzo pubblico "simulato":
200.34.11.103

CONNECTIVITY:

LAN -> DMZ: yes
DMZ -> LAN: no

WAN -> DMZ: yes (200.34.11.103:8000/biblionextgen2)
DMZ -> WAN: no

LAN -> LAN: yes
LAN -> WAN: yes



:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing ::

DMZ Setup

DMZ Port Setup ? help

Do you want to enable DMZ Port?

● Yes ○ No

IP Address: 192 .168 .2 .1

Subnet Mask: 255 .255 .255 .0

DHCP for DMZ Connected Computers ? help

○ Disable DHCP Server

● Enable DHCP Server

□ Enable LDAP information

Domain Name: netgearDMZ.com

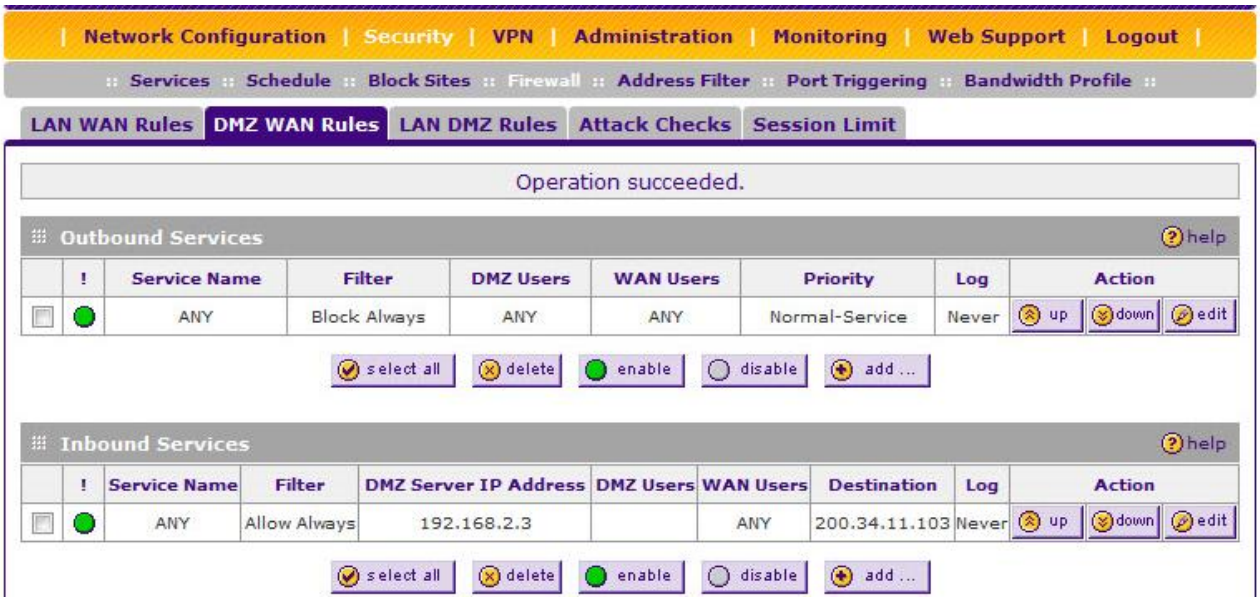
LDAP Server:

Starting IP Address: 192 .168 .2 .2

Search Base:

Ending IP Address: 192 .168 .2 .3

port: (leave blank for default port)



| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Block Sites :: Firewall :: Address Filter :: Port Triggering :: Bandwidth Profile ::
LAN WAN Rules | DMZ WAN Rules | LAN DMZ Rules | Attack Checks | Session Limit

Operation succeeded.

Outbound Services ? help

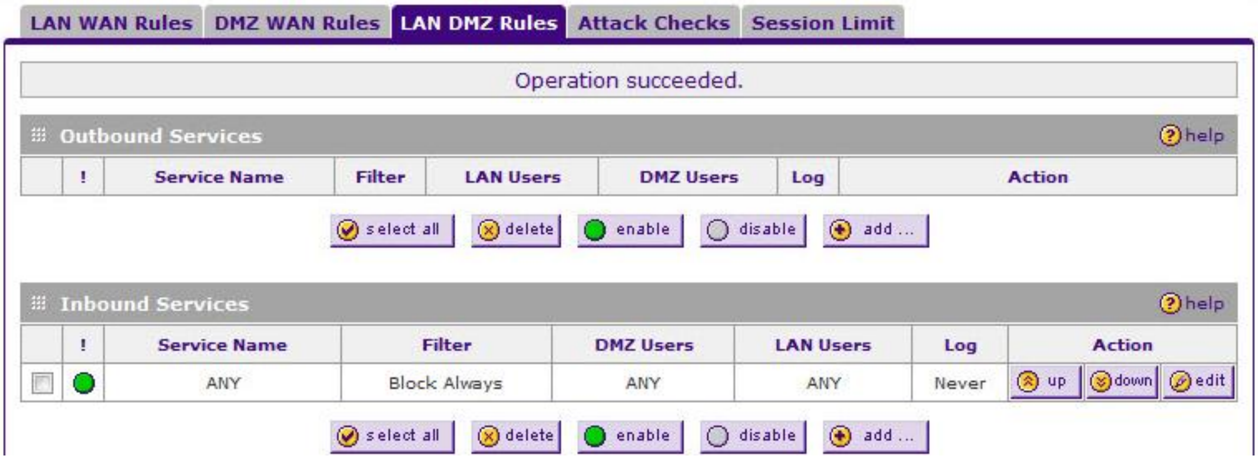
	!	Service Name	Filter	DMZ Users	WAN Users	Priority	Log	Action
□	●	ANY	Block Always	ANY	ANY	Normal-Service	Never	up down edit

select all | delete | enable | disable | add ...

Inbound Services ? help

	!	Service Name	Filter	DMZ Server IP Address	DMZ Users	WAN Users	Destination	Log	Action
□	●	ANY	Allow Always	192.168.2.3		ANY	200.34.11.103	Never	up down edit

select all | delete | enable | disable | add ...



LAN WAN Rules | DMZ WAN Rules | LAN DMZ Rules | Attack Checks | Session Limit

Operation succeeded.

Outbound Services ? help

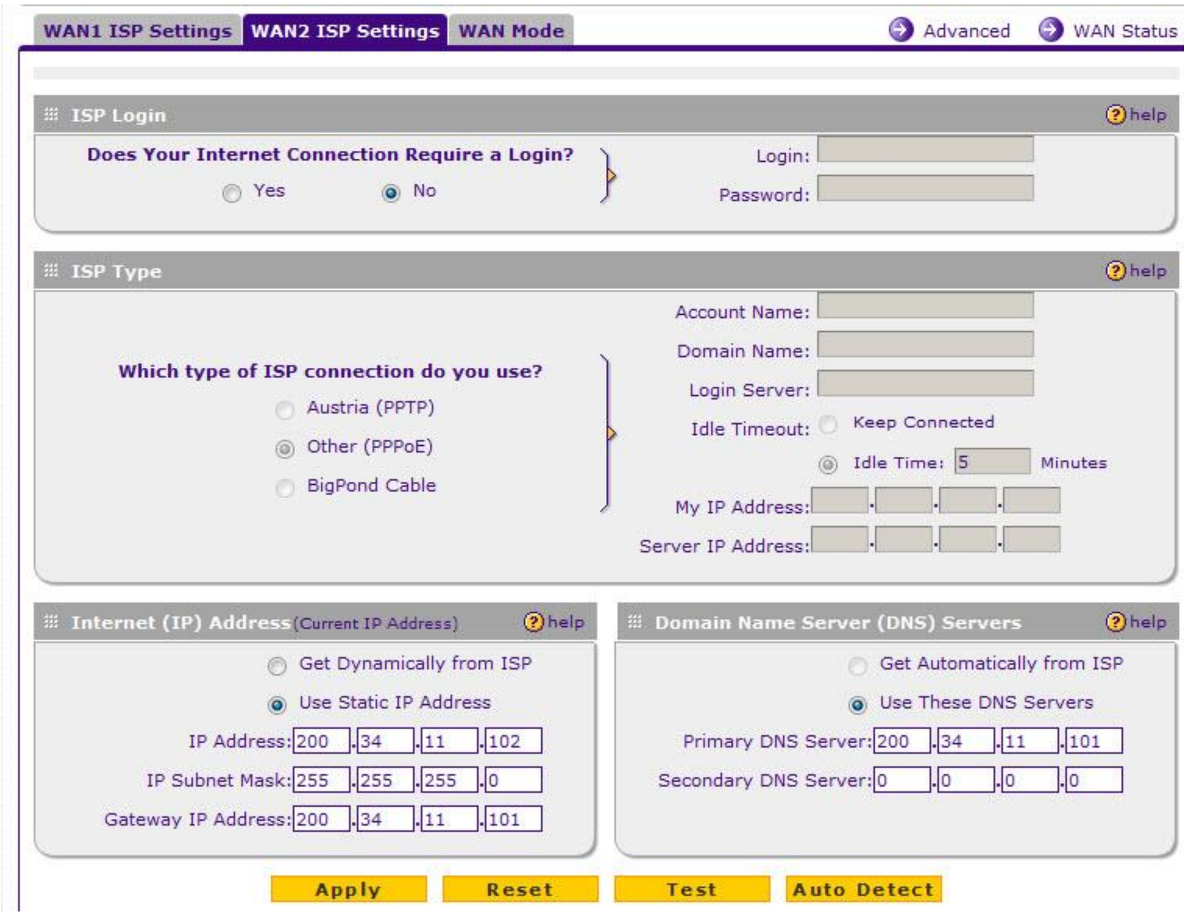
	!	Service Name	Filter	LAN Users	DMZ Users	Log	Action

select all | delete | enable | disable | add ...

Inbound Services ? help

	!	Service Name	Filter	DMZ Users	LAN Users	Log	Action
□	●	ANY	Block Always	ANY	ANY	Never	up down edit

select all | delete | enable | disable | add ...



ISP Login

Does Your Internet Connection Require a Login? ○ Yes ● No

Login:

Password:

ISP Type

Which type of ISP connection do you use?

○ Austria (PPTP)
● Other (PPPoE)
○ BigPond Cable

Account Name:

Domain Name:

Login Server:

Idle Timeout: ○ Keep Connected
● Idle Time: 5 Minutes

My IP Address: . . .

Server IP Address: . . .

Internet (IP) Address (Current IP Address)

○ Get Dynamically from ISP
● Use Static IP Address

IP Address: 200 . 34 . 11 . 102

IP Subnet Mask: 255 . 255 . 255 . 0

Gateway IP Address: 200 . 34 . 11 . 101

Domain Name Server (DNS) Servers

○ Get Automatically from ISP
● Use These DNS Servers

Primary DNS Server: 200 . 34 . 11 . 101

Secondary DNS Server: 0 . 0 . 0 . 0

3.1.1 Hping attack

200.34.11.101 started to send a continuous flow of large packets by using hping3 instrument with destination IP address equal to the WAN IP address of the Firewall (200.34.11.102). Firewall’s memory is immediately saturated.

In particular, we tried a Syn Flood attack after having blocked this kind of attack inside the firewall, using default rules:

```
hping3 -S -i u1 200.34.11.102
```

So we decided to verify if this firewall is able to block this kind of attack. In the “security section” we selected “block TCP flood” option: we can’t set anything else. We repeated the attack, but firewall’s memory is saturated again.

We wrote on NETGEAR’s forum, but none has been able to solve this problem, that is maybe a bug of this firewall.

Starting Hping with the DMZ IP address as target, we realized that the firewall does not send packets to the Server but its memory goes down anyway. This happens because we are using a stateful firewall, so it does not send any packet to the destination until it receives the last “ack” during three-way-handshake.

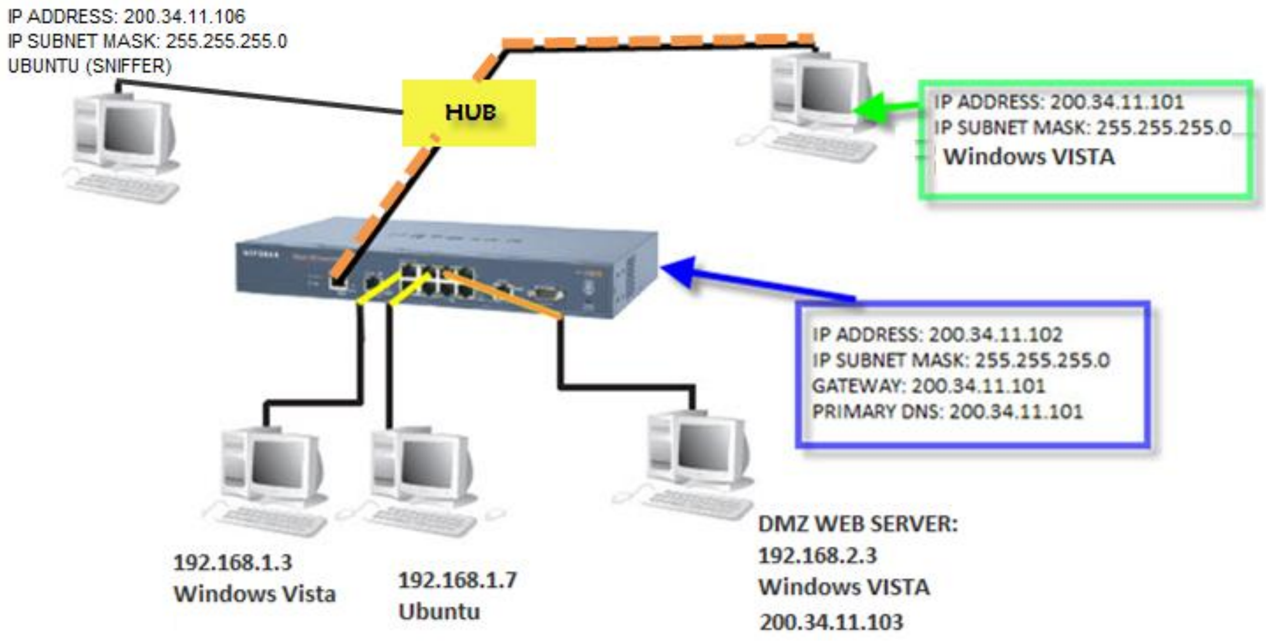
CONCLUSION: this firewall does not block Hping attack.

3.1.2 Port Scan

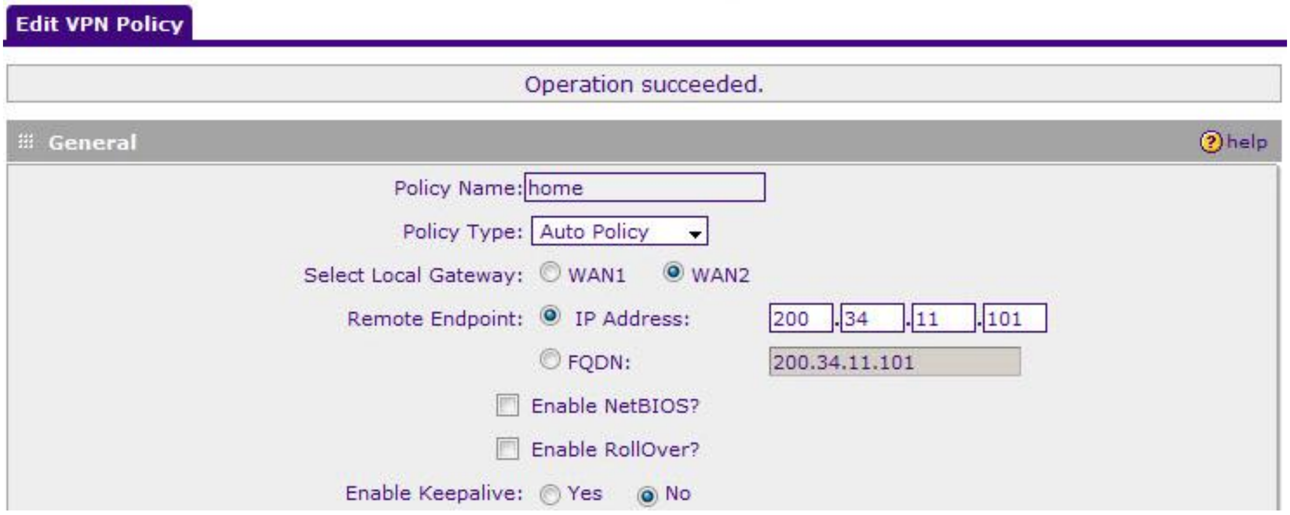
Firewall logs external port scans but it doesn't block them. We obtained the list of all open ports on WAN interface and the uptime.

Chapter 4: VPN

4.1 VPN Configuration


IP ADDRESS: 200.34.11.106
IP SUBNET MASK: 255.255.255.0
UBUNTU (SNIFFER)
HUB
IP ADDRESS: 200.34.11.101
IP SUBNET MASK: 255.255.255.0
Windows VISTA
IP ADDRESS: 200.34.11.102
IP SUBNET MASK: 255.255.255.0
GATEWAY: 200.34.11.101
PRIMARY DNS: 200.34.11.101
192.168.1.3
Windows Vista
192.168.1.7
Ubuntu
DMZ WEB SERVER:
192.168.2.3
Windows VISTA
200.34.11.103

We setup VPN using on the external host “Netgear VPN client software”. As far as the firewall concerns, the configuration is the following:



Operation succeeded.

Policy Name: home

Policy Type: Auto Policy

Select Local Gateway: ○ WAN1 ● WAN2

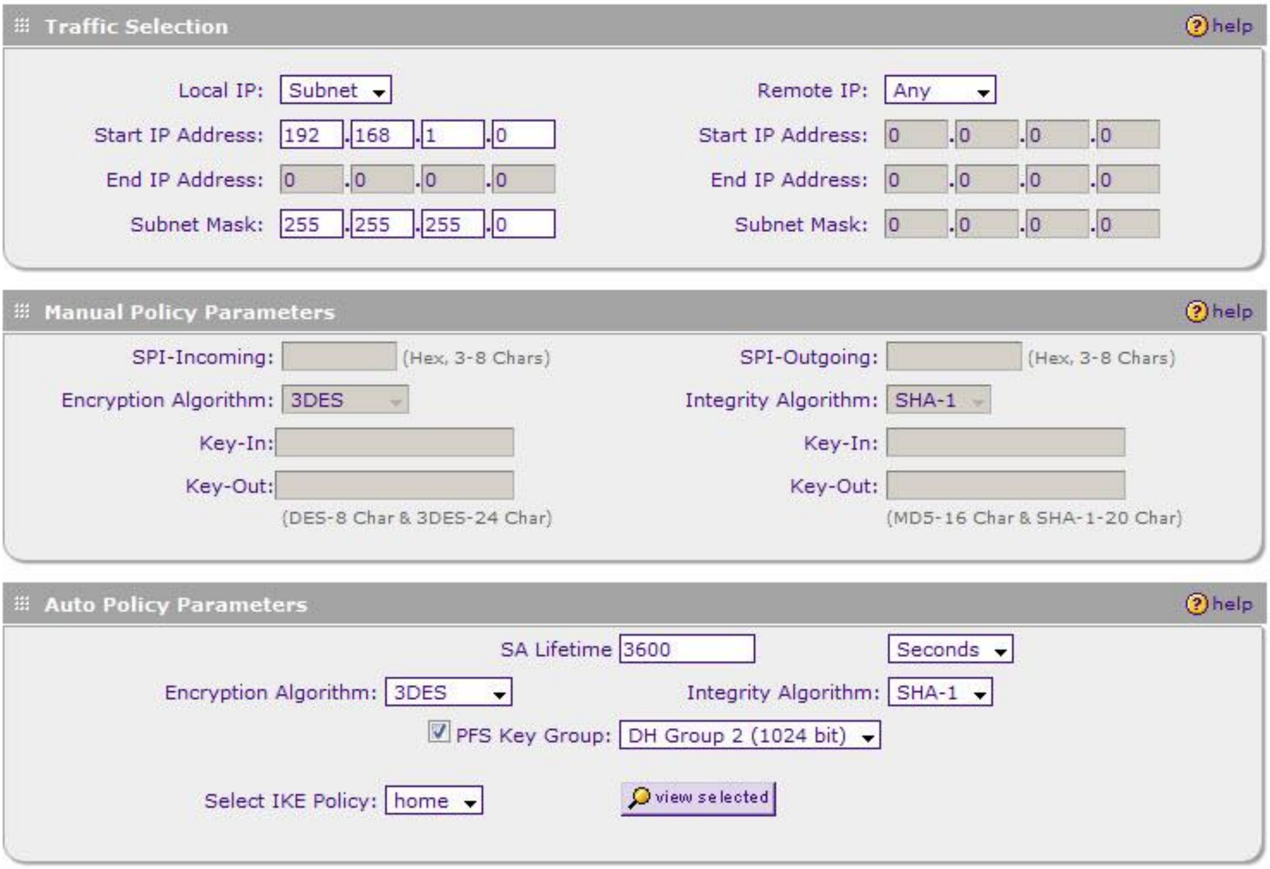
Remote Endpoint: ● IP Address: 200 . 34 . 11 . 101

○ FQDN: 200.34.11.101

□ Enable NetBIOS?

□ Enable RollOver?

Enable Keepalive: ○ Yes ● No



Traffic Selection

Local IP: Subnet

Start IP Address: 192.168.1.0

End IP Address: 0.0.0.0

Subnet Mask: 255.255.255.0

Remote IP: Any

Start IP Address: 0.0.0.0

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Manual Policy Parameters

SPI-Incoming: (Hex, 3-8 Chars)

Encryption Algorithm: 3DES

Key-In:

Key-Out:

(DES-8 Char & 3DES-24 Char)

SPI-Outgoing: (Hex, 3-8 Chars)

Integrity Algorithm: SHA-1

Key-In:

Key-Out:

(MD5-16 Char & SHA-1-20 Char)

Auto Policy Parameters

SA Lifetime 3600 Seconds

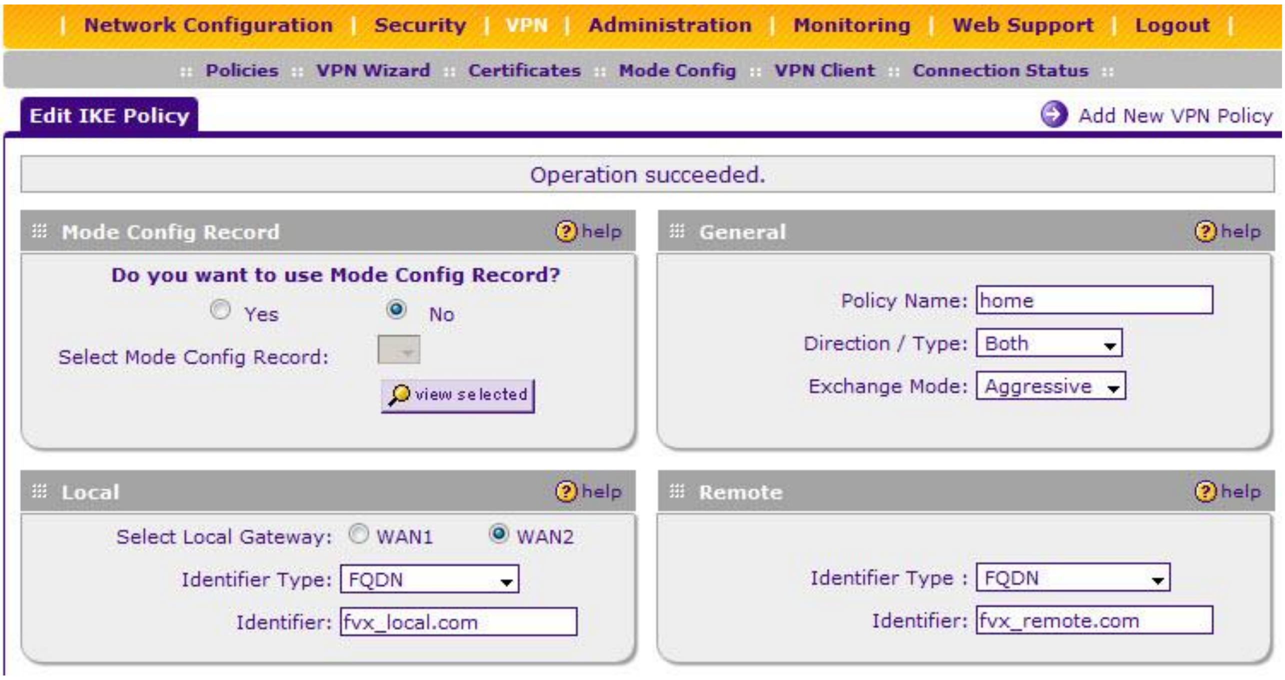
Encryption Algorithm: 3DES

Integrity Algorithm: SHA-1

☑ PFS Key Group: DH Group 2 (1024 bit)

Select IKE Policy: home

help
help
help
view selected



| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Policies :: VPN Wizard :: Certificates :: Mode Config :: VPN Client :: Connection Status ::
Edit IKE Policy
Add New VPN Policy
help
help
help
help
view selected

Operation succeeded.

Mode Config Record

Do you want to use Mode Config Record?

○ Yes ● No

Select Mode Config Record:

General

Policy Name: home

Direction / Type: Both

Exchange Mode: Aggressive

Local

Select Local Gateway: ○ WAN1 ● WAN2

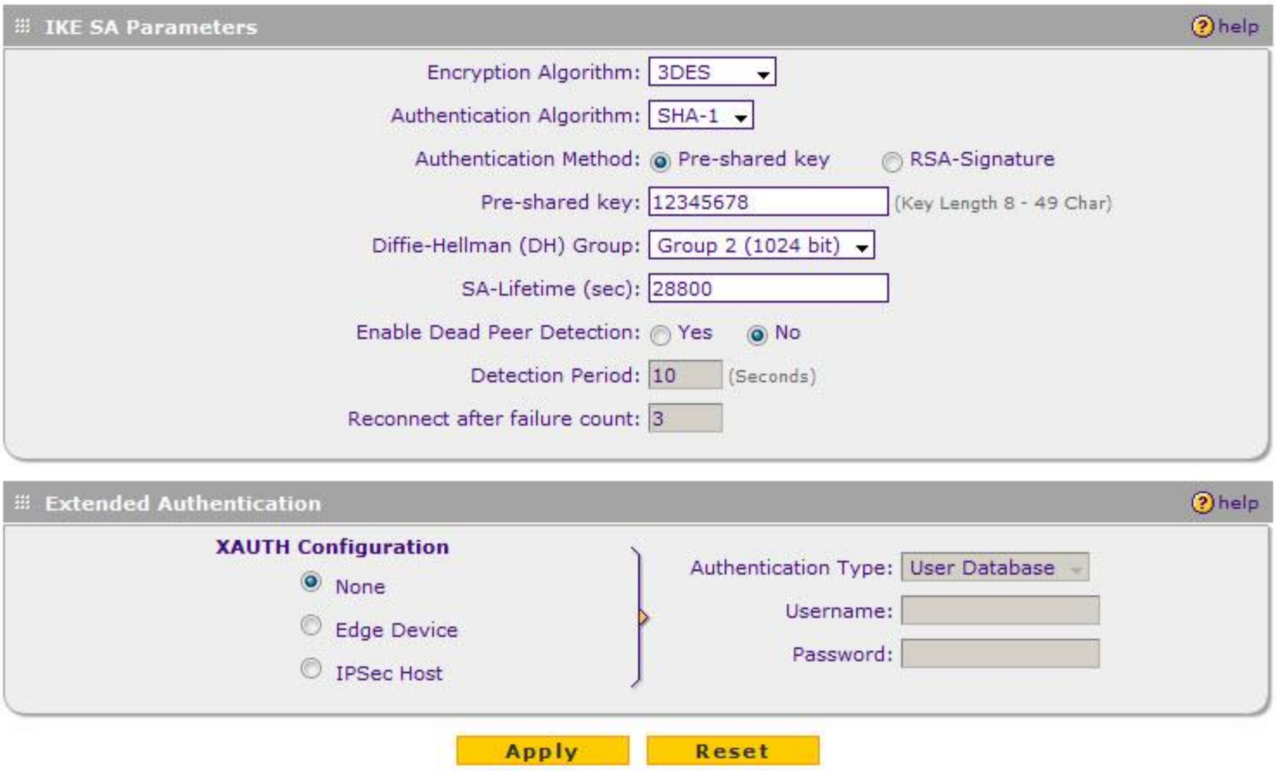
Identifier Type: FQDN

Identifier: fvx_local.com

Remote

Identifier Type : FQDN

Identifier: fvx_remote.com



IKE SA Parameters ? help

Encryption Algorithm: 3DES

Authentication Algorithm: SHA-1

Authentication Method: ● Pre-shared key ○ RSA-Signature

Pre-shared key: 12345678 (Key Length 8 - 49 Char)

Diffie-Hellman (DH) Group: Group 2 (1024 bit)

SA-Lifetime (sec): 28800

Enable Dead Peer Detection: ○ Yes ● No

Detection Period: 10 (Seconds)

Reconnect after failure count: 3

Extended Authentication ? help

XAUTH Configuration

● None

○ Edge Device

○ IPSec Host

Authentication Type: User Database

Username:

Password:

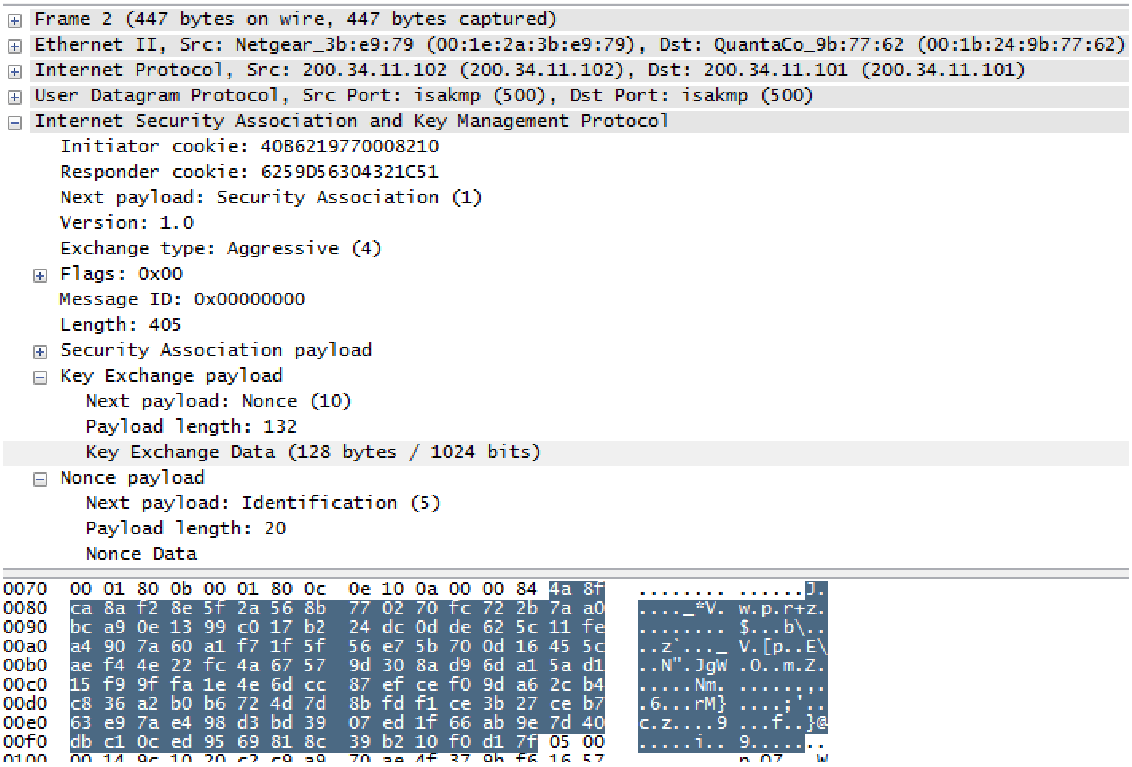
Apply Reset

4.1.1 Sniffing VPN startup

Our VPN has been built over IPSec. The encryption algorithm used is 3DES and the authentication method is based on a pre-shared key.

200.34.11.106 is connected to an hub so it can listen all traffic exchanged between the firewall and the external host. To say the truth, the hub in not necessary: in fact, if we had a switch we could still sniff by doing arp poisoning (for example by ETTERCAP).

The result of this experiment is that we sniffed the conversation and also the password exchange, but all the conversation is ciphered, so an attacker can only try the “cipher-text only attack”.



```
⊞ Frame 2 (447 bytes on wire, 447 bytes captured)
⊞ Ethernet II, Src: Netgear_3b:e9:79 (00:1e:2a:3b:e9:79), Dst: QuantaCo_9b:77:62 (00:1b:24:9b:77:62)
⊞ Internet Protocol, Src: 200.34.11.102 (200.34.11.102), Dst: 200.34.11.101 (200.34.11.101)
⊞ User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
⊟ Internet Security Association and Key Management Protocol
    Initiator cookie: 40B6219770008210
    Responder cookie: 6259D56304321C51
    Next payload: Security Association (1)
    Version: 1.0
    Exchange type: Aggressive (4)
  ⊞ Flags: 0x00
    Message ID: 0x00000000
    Length: 405
  ⊞ Security Association payload
  ⊟ Key Exchange payload
      Next payload: Nonce (10)
      Payload length: 132
      Key Exchange Data (128 bytes / 1024 bits)
  ⊟ Nonce payload
      Next payload: Identification (5)
      Payload length: 20
      Nonce Data

0070  00 01 80 0b 00 01 80 0c  0e 10 0a 00 00 84 4a 8f   ........ ......J.
0080  ca 8a f2 8e 5f 2a 56 8b  77 02 70 fc 72 2b 7a a0   ....._*V. w.p.r+z.
0090  bc a9 0e 13 99 c0 17 b2  24 dc 0d de 62 5c 11 fe   ........ $...b\..
00a0  a4 90 7a 60 a1 f7 1f 5f  56 e7 5b 70 0d 16 45 5c   ..z`...._ V.[p..E\
00b0  ae f4 4e 22 fc 4a 67 57  9d 30 8a d9 6d a1 5a d1   ..N".JgW .0..m.Z.
00c0  15 f9 9f fa 1e 4e 6d cc  87 ef ce f0 9d a6 2c b4   .....Nm. ......,.
00d0  c8 36 a2 b0 b6 72 4d 7d  8b fd f1 ce 3b 27 ce b7   .6...rM} ....;'..
00e0  63 e9 7a e4 98 d3 bd 39  07 ed 1f 66 ab 9e 7d 40   c.z....9 ...f..}@
00f0  db c1 0c ed 95 69 81 8c  39 b2 10 f0 d1 7f 05 00   .....i.. 9.......
0100  00 14 9c 10 20 c2 c9 a9  70 ae 4f 37 9b f6 16 57            p.O7   W
```