TELECOM | DATACENTER

Idéias que se justificam

Firewall Fortinet - Fortigate

Número do Documento: Firewall Fortinet - Fortigate
Nível da Versão: 1.0
Nível da Revisão: 1.0
Data de criação: 20 de março de 2010.

Data da ultima publicação: 10 de junho de 2009.

Acesso Interno-Restrito as áreas de Engenharia e Operações.

Informação de Copyright

Histórico de Mudanças

Revisão	Data	Autor	Tipo/Versão	Descrição da Versão / Revisão
01	19/04/2010	Laurence Stendard	Tipo / 01	Versão Inicial
02	03/12/2010	Laurence Stendard	Tipo / 02	Revisão

Histórico de Aceite e Testes

Freqüência dos Testes			Semestral/Anual	
Revisão	**Data**	**Realizador**	**Data do Próximo Teste**	**Resultado**
01		Nome do Realizador do Teste		Satisfatório/Insatisfatório/ Insuficiente

Freqüência dos Testes			Semestral/Anual	
Revisão	**Data**	**Realizador**	**Data do Próximo Teste**	**Resultado**

Colaboradores

- Fabiana Rett
- Priscilla Dell' Agnolo
- Everton da Silva Marques

Lista de Distribuição

- Engenharia Datacenter e Telecom
- GPP
- Incidentes
- Implantação Datacenter e Telecom
- Sistemas & TI

Índice

1 Objetivo.....10
2 Introdução.....10
3 Equipamento de Testes.....10
4 Instalação.....11
5 Configurações Básicas.....12
5.1 Senha do Administrador.....12
5.2 Administrador Remoto – TACACS+.....13
5.2.1 Servidor TACACS+.....13
5.2.2 Grupo a ser Autenticado no TACACS+.....15
5.2.3 Administrador a ser Autenticado no TACACS+.....16
5.2.4 Verificação de Acessos.....17
5.3 Host Name.....18
5.4 Data e Hora.....18
5.5 Timeout da Console.....19
5.6 Interfaces.....20
5.6.1 VLANs.....21
5.6.2 Endereços Secundários.....22
5.6.3 Forçar Velocidade e Modo de Operação.....23
5.6.4 Verificar Modo de Operação das Interfaces.....24
5.6.5 Agregação de Portas – 802.3AD.....24
5.7 Rotas.....26
5.8 DNS.....27
6 Firewall.....27
6.1 Regras.....27
6.1.1 Regra Default.....28
6.2 NAT.....29
6.2.1 Exemplo 1 – Virtual IP (VIP) - NAT de Entrada.....29
6.2.2 Exemplo 2 – IP Pool – NAT de Saída.....31
6.2.3 Exemplo 3 - Virtual IP (VIP) - NAT de Saída.....34
6.2.4 Exemplo 4 - Central NAT Table - NAT de Saída.....37
6.2.5 Exemplo 5 - Vários NAT de Entrada na Mesma Regra.....41
6.3 Session/Service Timeout.....42
7 Log.....43

7.1 Configuração.....44
7.2 Filtro.....46
7.3 SYSLOG – Log Remoto.....47
7.3.1 Exemplo de Log de uma Sessão de Firewall.....47
7.3.2 Exemplo de Log de uma Sessão de IPS.....48
7.3.3 Exemplo de Configuração de Servidor syslog-ng.....48
8 Alta Disponibilidade – High Availability (HA).....49
8.1 MAC Address em cluster HA.....52
8.2 Verificação de Status Através da CLI.....53
9 VPN IPSEC – Client-to-Site.....54
9.1 VPN IPSEC – Client-to-Site – Método 1.....54
9.1.1 Servidor TACACS+.....54
9.1.2 Grupo de Usuários da VPN IPSEC.....57
9.1.3 Fase 1.....58
9.1.4 Fase 2.....59
9.1.5 Endereços da Rede Interna e Range dos Remote Clients.....60
9.1.6 Regra de VPN.....61
9.1.7 DHCP para Remote Clients.....63
9.1.8 Instalação do FortiClient Endpoint Security Application.....64
9.2 VPN IPSEC – Client-to-Site – Método 2.....74
9.3 Monitoração dos Acessos à VPN IPSec.....76
10 VPN SSL - Client-to-Site.....76
10.1 Acesso no Modo Web.....76
10.1.1 Editar o Address Range SSLVPN_TUNNEL_ADDR1.....76
10.1.2 Habilitar SSL.....77
10.1.3 Criar Portal.....78
10.1.4 Criar conta e grupo para os usuários da SSL VPN.....80
10.1.5 Criar regras para permitir o acesso externo à VPN SSL.....82
10.1.6 Acessar a VPN através do browser.....84
10.1.7 Exemplo de Acesso RDP.....86
10.1.8 Configuração Opcional: Alterar Porta de Acesso à SSL VPN.....89
10.1.9 Monitoração dos Acessos.....89
10.2 Acesso no Modo Túnel.....90
10.3 Monitoração de Acessos.....104
11 VPN IPSEC – Site-to-Site.....104
11.1 Fase 1.....104
11.2 Fase 2.....105
11.3 Regras.....107
11.4 Monitoração.....108

12 IPS.....110
12.1 IPS Sensor.....110
12.2 Filtro.....111
12.3 Regra de Firewall.....112
12.4 Log de Ataques.....113
12.5 Assinaturas de Ataques Pré-definidas.....115
12.6 Alterar o Comportamento de uma Assinatura e White-list.....115
12.7 Criar uma Assinatura Customizada.....119
12.8 Configurar Horário de Atualização de Assinaturas.....122
13 DoS Sensor.....123
13.1 Syn Flood.....123
13.2 Limite de Sessões Por Destino.....126
13.3 Port Scan.....128
11 Backup e Restore.....130
13.4 Backup Através da CLI.....131
14 OSPF.....131
14.1 Configuração VIA CLI.....131
14.2 Monitoração do OSPF via CLI.....132
14.2.1 Rotas Aprendidas.....132
14.2.2 Interfaces.....132
14.2.3 Neighbors.....133
14.2.4 Status.....133
14.2.5 Executar Clear no Processo OSPF.....133
15 SNMP.....134
16 VDOM.....137
16.1 Habilitar VDOM.....137
16.2 Criar VDOM.....138
16.3 Editar Limites Para o VDOM.....139
16.4 Adicionar Interfaces ao VDOM.....140
16.5 Adicionar Administradores ao VDOM.....142
16.6 VDOM Root e VDOM Global.....143
16.7 Remover VDOM.....144
16.8 Desabilitar VDOM.....145
16.9 Command Line – CLI.....145
17 Operação no Modo Transparent/Bridge.....146
17.1 Spanning Tree.....147
17.2 Multicast.....147
17.3 Troubleshooting e Best Practices – KB FD30087.....148
18 Firmware Upgrade.....151

19 Performance.....153
19.1 Ping Flood.....153
19.2 IPerf.....153
19.3 Web Attack.....153
19.4 Syn Flood – IP Fixo no Atacante.....154
19.5 Syn Flood – Spoofed Address no Atacante – Sem Limite de Sessões.....154
19.6 Syn Flood – Spoofed Address no Atacante – Com Limite de Sessões.....155
20 Troubleshooting.....156
20.1 Ping Extendido.....156
20.2 Captura de Pacotes.....156
20.3 Listar Sessões.....157
20.4 Debug de IPSec VPN.....159
20.5 Debug de Sessões.....160
21 Command Line Interface (CLI) – Comandos Úteis.....161
21.1 grep.....161
21.2 show full-configuration.....162
21.3 show full-configuration <config block>.....162
21.4 get system performance status.....163
21.5 get system performance top.....163
21.6 get hardware status.....164
21.7 get system status.....164
21.8 get system interface physical.....164
21.9 show system interface.....165
21.10 diagnose hardware deviceinfo nic <port>.....166
21.11 diagnose ip arp list.....167
21.12 diagnose system kill 9.....167
21.13 diag test auth tacacs+ <server_name> <username> <password>.....167
21.14 get router info routing-table details.....168
21.15 get system session status.....168
21.16 get system session list.....168
21.17 get system arp.....169
21.18 show firewall policy.....169
21.19 show firewall address.....170
21.20 show firewall central-nat.....170
21.21 get firewall service custom/group/predefined.....170
21.22 execute update-ips.....171

21.23 get system auto-update status.....171
21.24 execute factoryreset.....171
22 Diversos.....171
22.1 Firewall e Reverse Path.....171
22.2 Encontrar Regras que Usam um Determinado Address ou Address Group 172
22.3 Encontrar Objetos que usam uma determinada interface.....172
22.4 Configurar Syslog pela CLI.....173
22.5 Recuperar a password do Admin.....173
22.6 FortiGate 200B – Converter Interfaces do Switch para Interfaces L3 173
22.7 Creating custom IPS signature to detect.....175
22.8 Creating custom IPS signature to detect a pattern rate - example to detect a Brute-force attack.....175
Apêndice I - Autenticação no Windows Active Directory Através de LDAP.....176
Apêndice II - Autenticação no Windows Active Directory Através de LDAP over SSL (LDAPS).....181
Apêndice III - Autenticação no Windows Active Directory com Restrição de Acesso a um Grupo no AD.....208

1 Objetivo

O presente documento apresenta as funcionalidades básicas do UTM Fortigate 51B e do seu firmware.

São apresentados ainda os procedimentos de configuração e operação do referido equipamento

2 Introdução

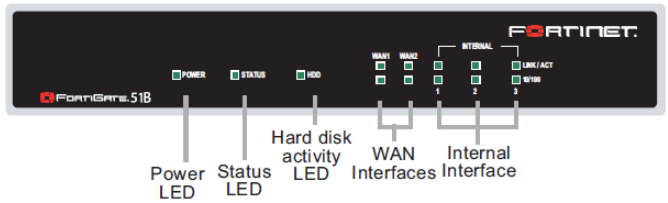
O Fortigate 50B é um UTM desenvolvido pela empresa Fortinet. Dentre as suas principais funcionalidades/características estão:

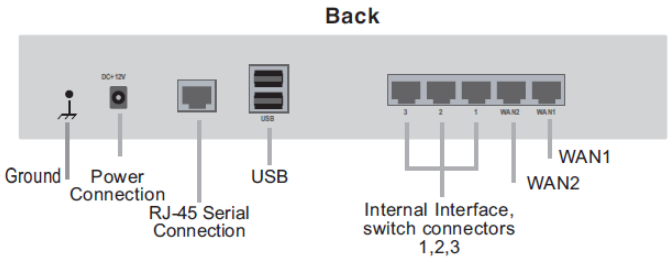
- Firewall;
- IDS/IPS (deteção baseada em assinaturas e comportamento de rede);
- VPN gateway IPsec e SSL;
- Roteador com suporte aos protocolos RIP, OSPF, BGP e ISIS;
- Virtualização completa através do recurso de Virtual Domains (VDOM);
- Operação no modo NAT (roteamento) e Transparent (bridge);
- Suporte a IPv6;
- Aceita gerenciamento centralizado e/ou individual;
- Configuração através de interface web e console (local/ssh).

3 Equipamento de Testes

Equipamento utilizado nos testes:

- Fortigate 51B
- Firmware FortiOS versão 4.0 MR2
- Interfaces: 2 interfaces 100BaseT modo router - Wan1 e Wan2) e 3 interfaces 100BaseT modo switch.
- URL: http://www.fortinet.com/products/fortigate/50B.html

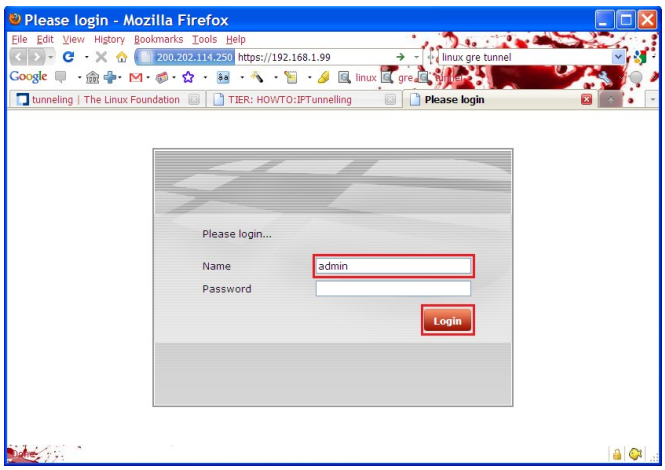




4 Instalação

Na configuração default os firewalls Fortigate possuem o endereço 192.168.1.99 (máscara 255.255.255.0) configurado na sua interface interna. Para acessar a Web Interface do equipamento deve-se conectar uma workstation à esta interface, configurar nesta workstation um endereço da rede 192.168.1.0/24 e acessar a URL https://192.168.1.99.

Na tela de login preencher o campo Name com *admin* e pressionar o botão Login (o campo Password deve ser deixado "em branco").



Outra forma de se acessar o equipamento é conectando-se um cabo "RJ-45 – DB9" (que acompanha o firewall) à sua interface RJ-45 serial. O software de console deve ser configurado com: velocidade = 9600, bits = 8, paridade = none, stop bit = 1. Esta conexão permitirá ao operador obter acesso à Command Line Interface do equipamento (CLI).

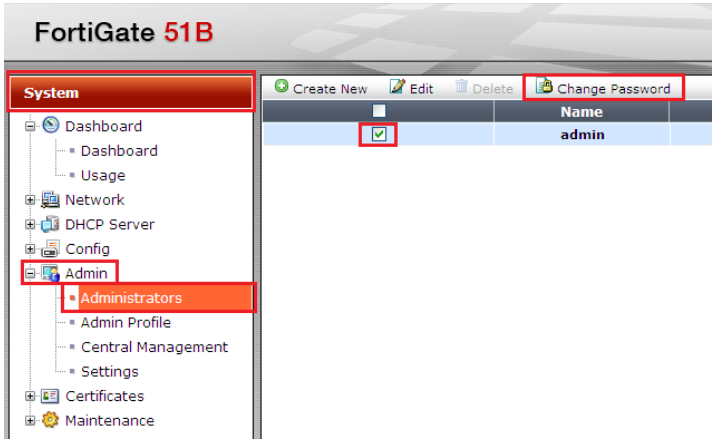
Ao receber o prompt de login deve-se digitar *admin* e apenas pressionar enter no prompt da password (não há password inicialmente definida para o usuário admin).

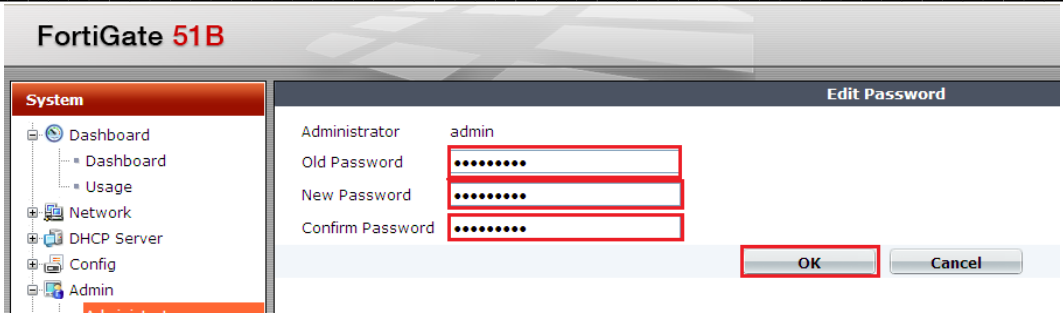
O processo de instalação com os passos específicos de cada modelo de Fortigate é descrito no Quick Start Guide. O Quick Start Guide de cada modelo de firewall está disponível no link: http://docs.fortinet.com/fgt_qsg.html

5 Configurações Básicas

5.1 Senha do Administrador

Antes de colocar o equipamento em operação deve-se definir uma senha para o administrador (o default é sem senha).

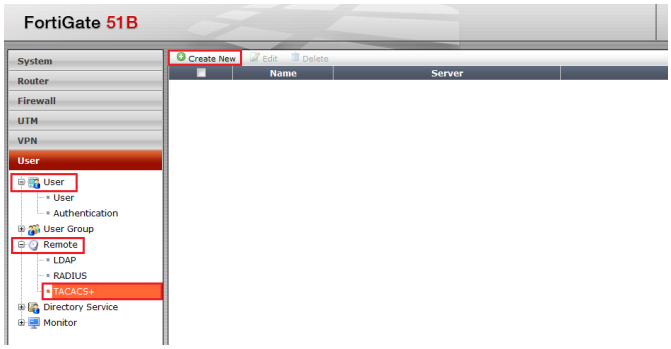


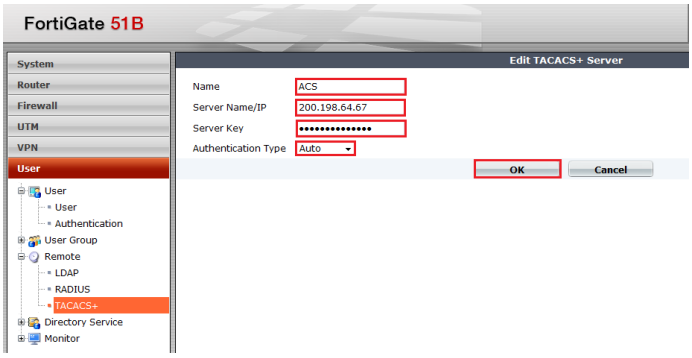


5.2 Administrador Remoto – TACACS+

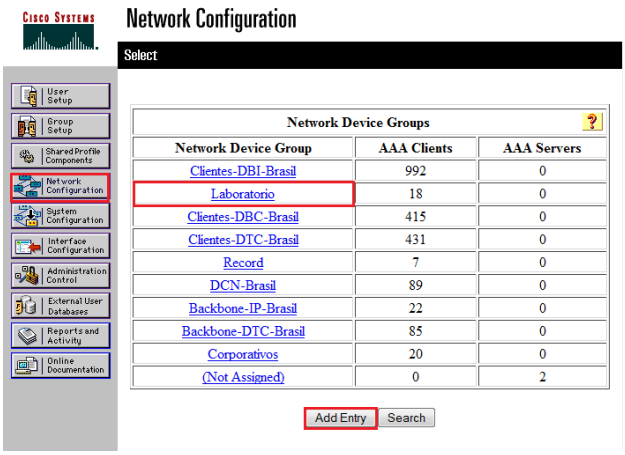
O FortiOS permite que os administradores do equipamento sejam autenticados através de TACACS+. A configuração para este tipo de autenticação é apresentada nos itens a seguir.

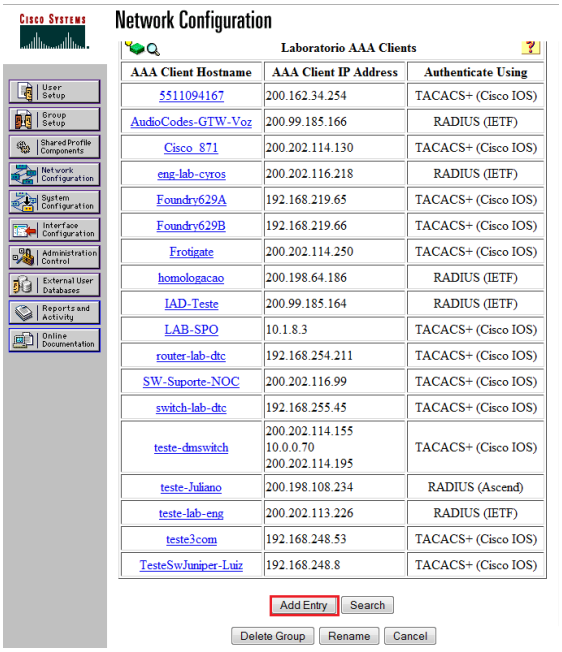
5.2.1 Servidor TACACS+

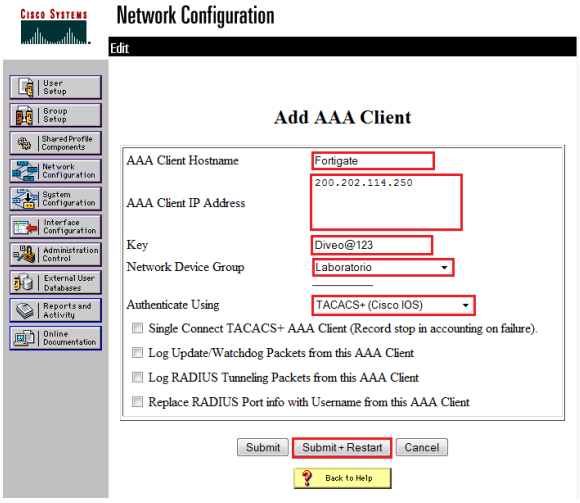




As telas abaixo apresentam as configurações realizadas no Cisco ACS:



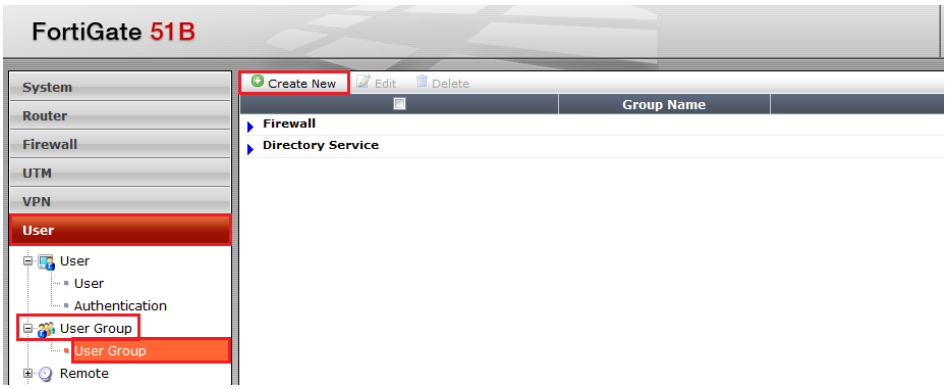


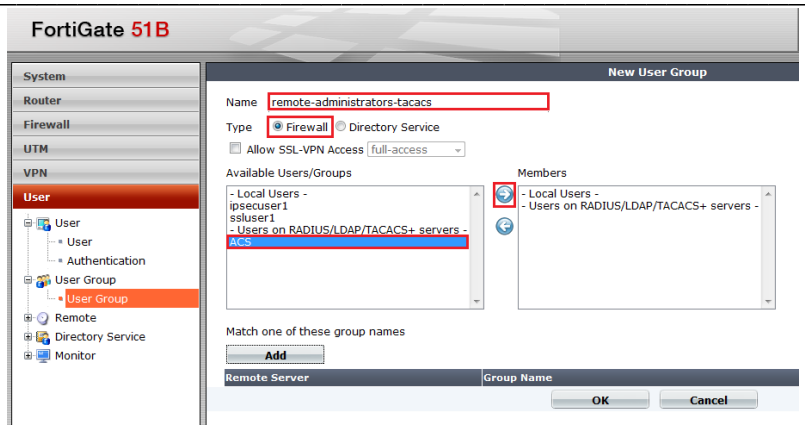


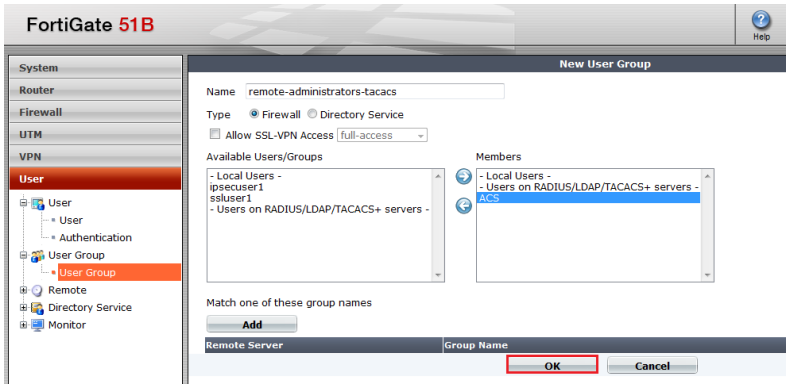
*Obs: O campo "Key" deve ser preenchido com o mesmo valor usado no campo "Server Key" da configuração do Fortigate.

5.2.2 Grupo a ser Autenticado no TACACS+

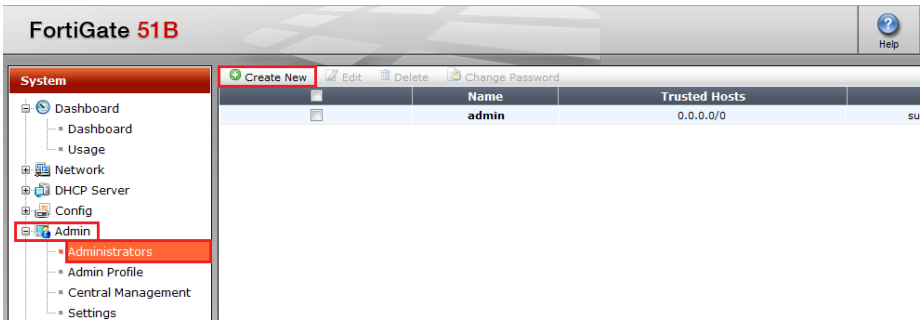
Criar grupo a ser autenticado no servidor Tacacs+ (Cisco ACS)

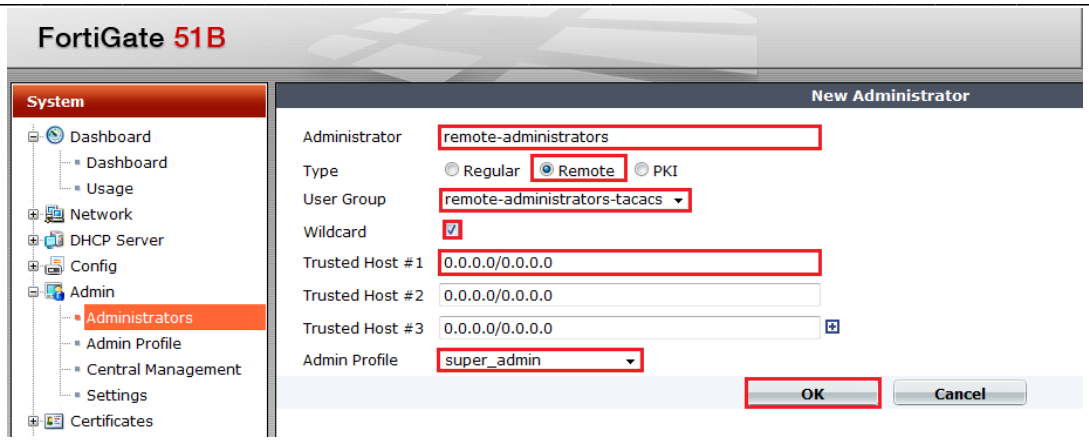






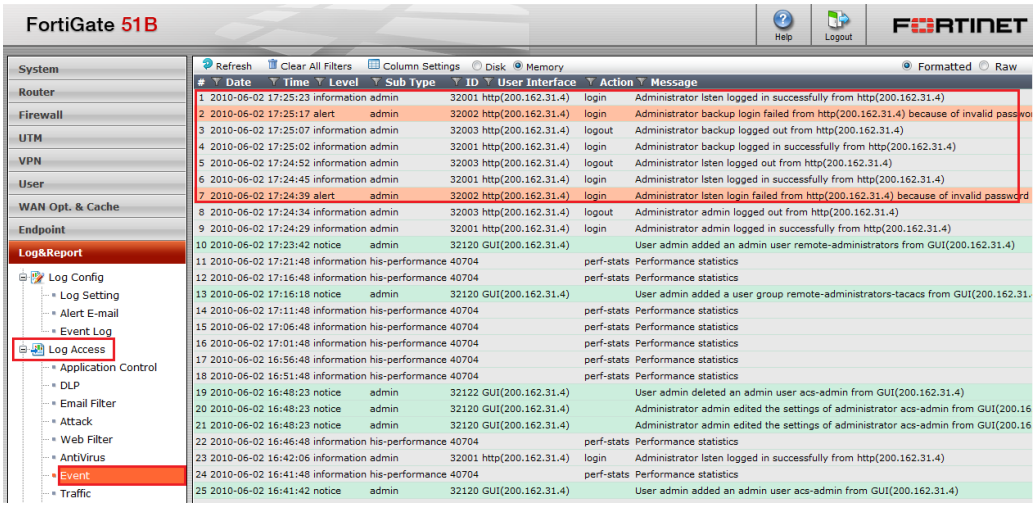
5.2.3 Administrador a ser Autenticado no TACACS+





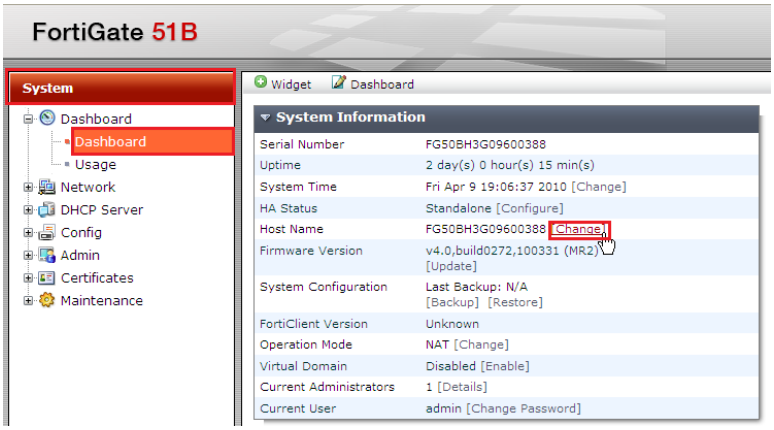
5.2.4 Verificação de Acessos

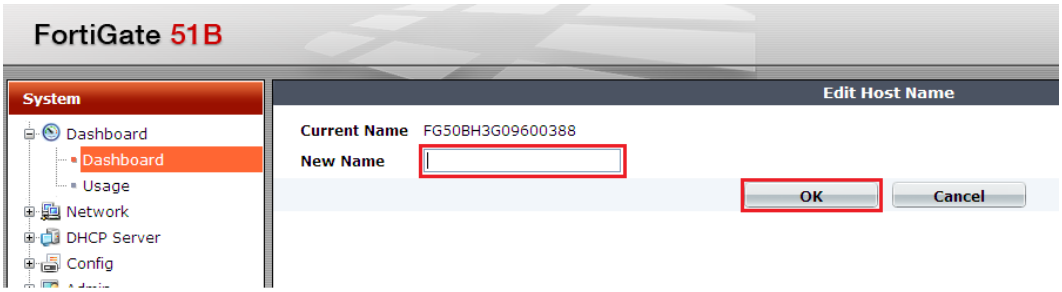
Os acessos dos administradores ao equipamento podem ser verificados através dos logs de eventos:



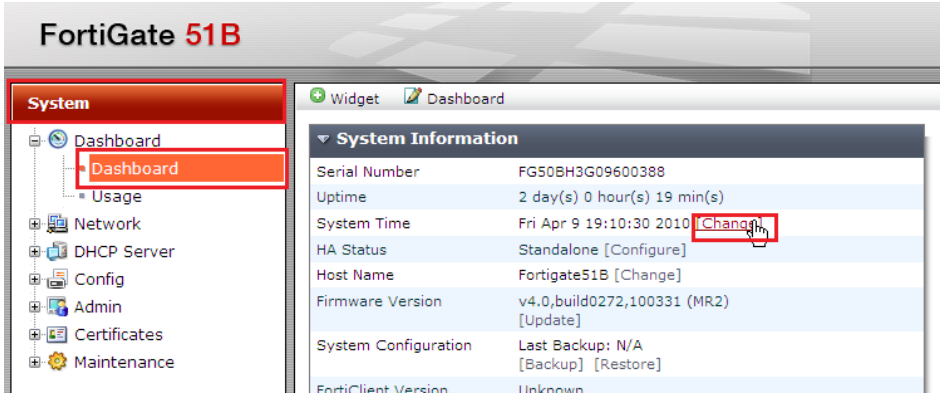
5.3 Host Name

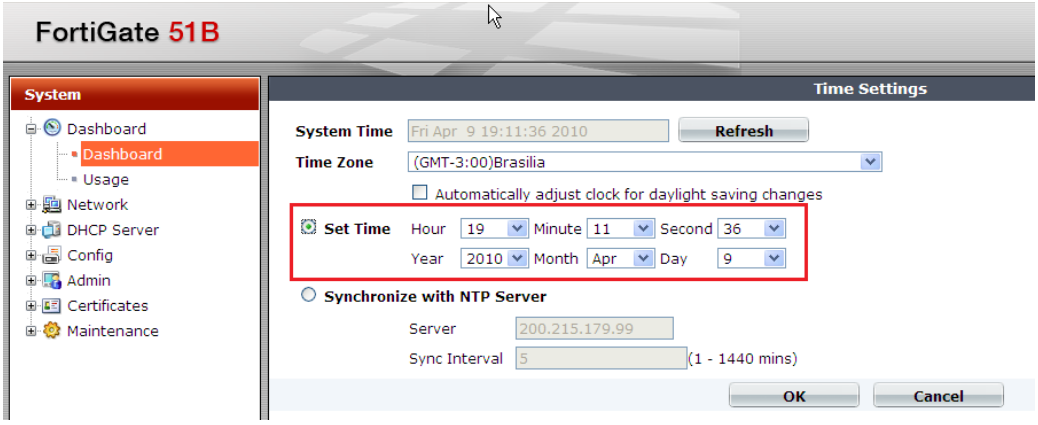
O host name pode alterado através do Dashboard.

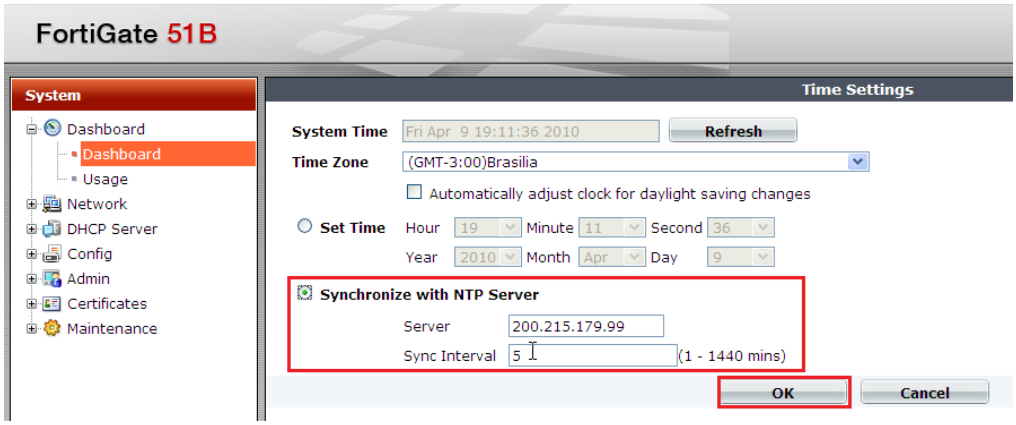




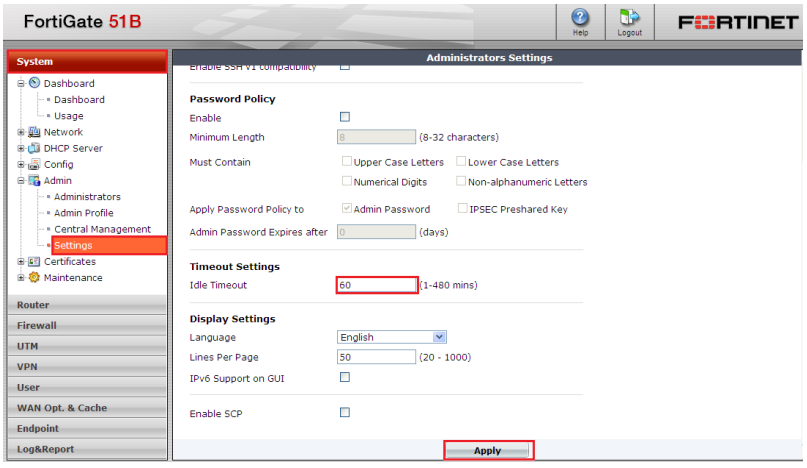
5.4 Data e Hora





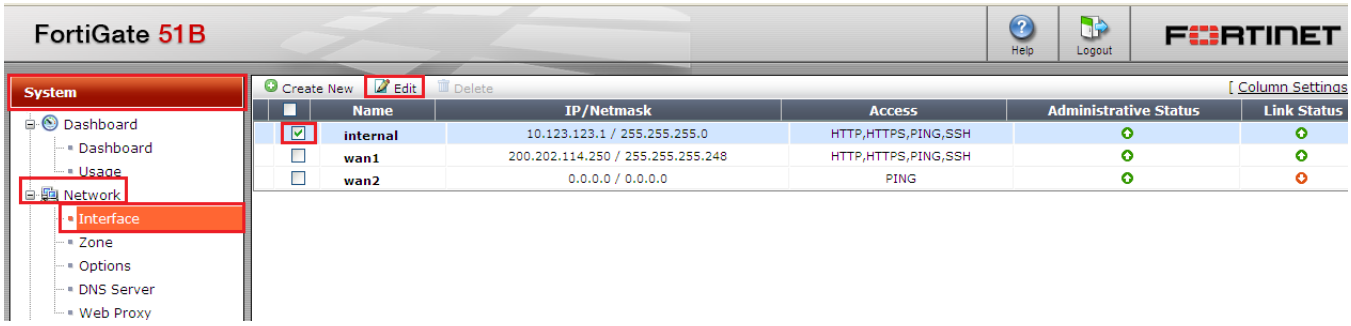


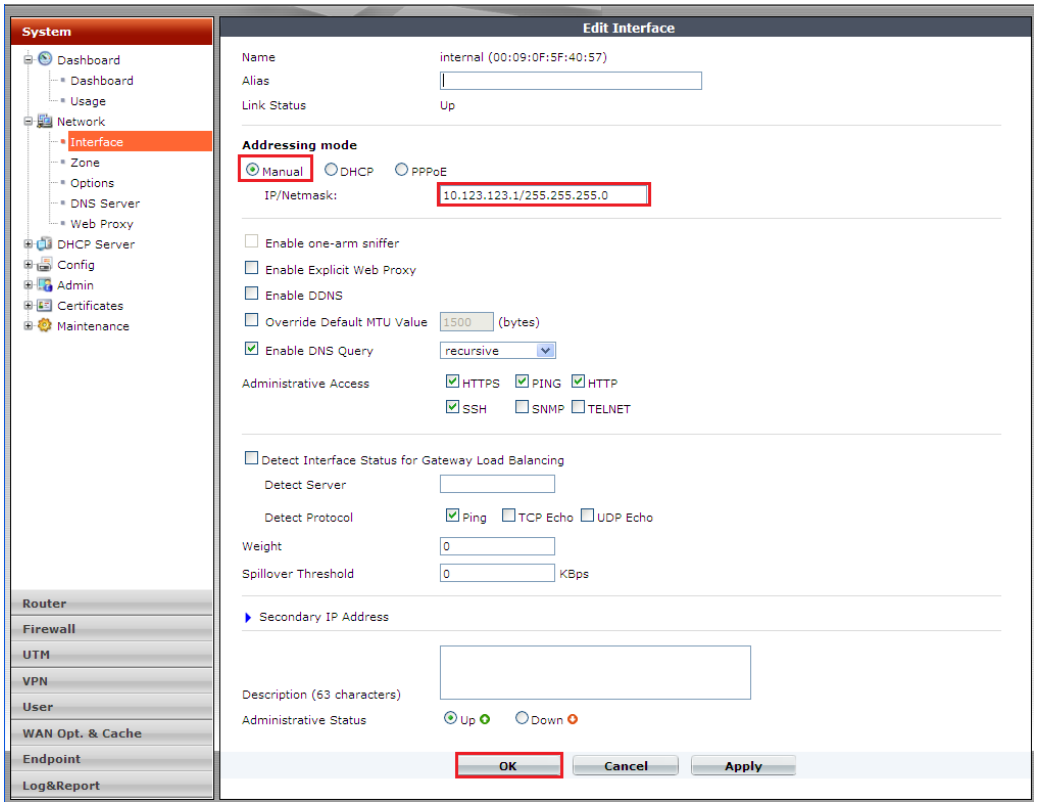
5.5 Timeout da Console



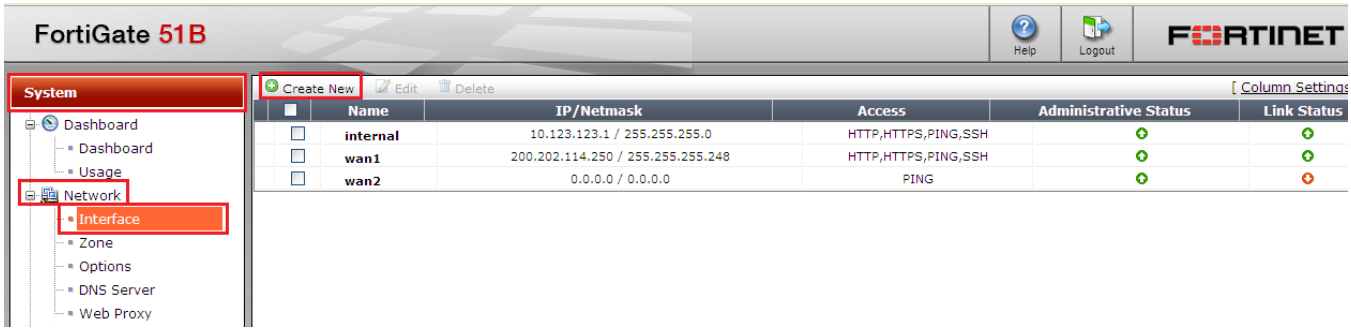
5.6 Interfaces

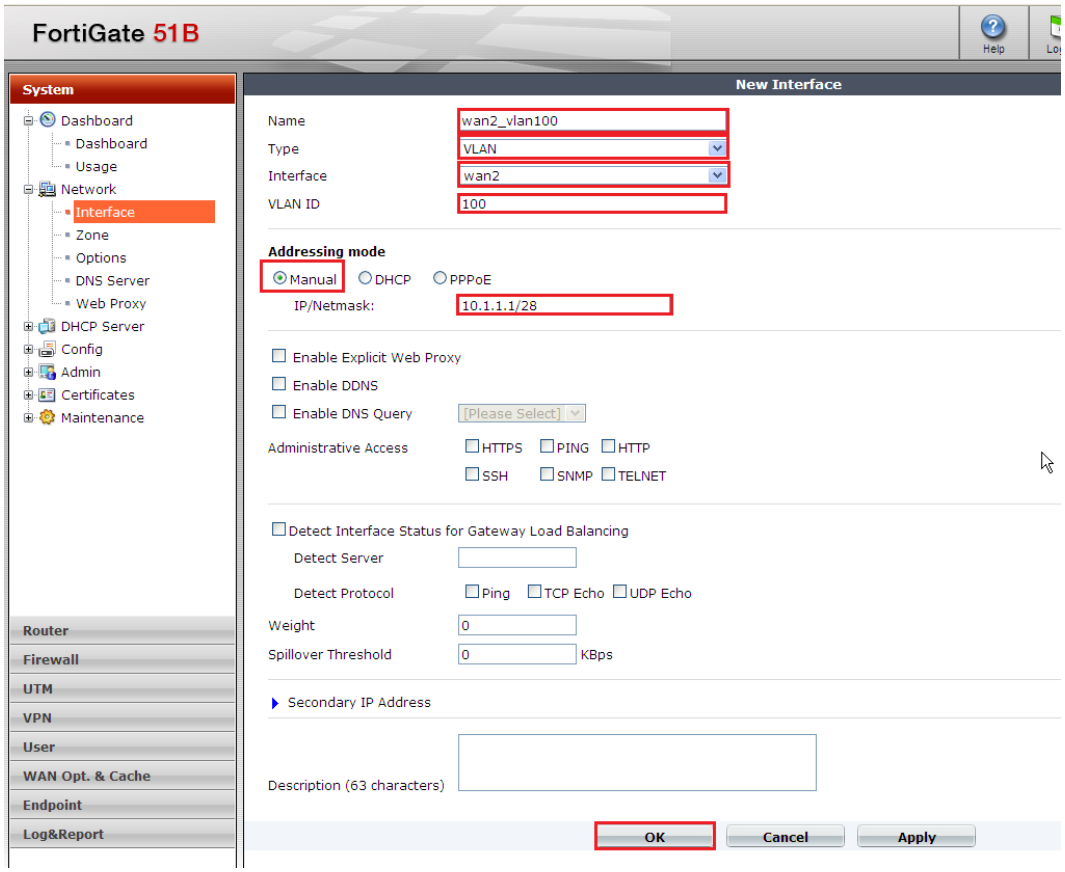
As configurações de interfaces são realizadas em Network -> Interface.





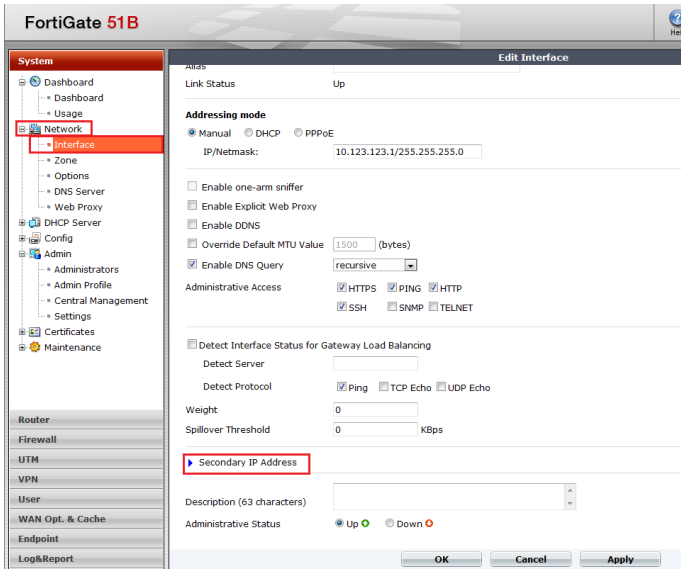
5.6.1 VLANs

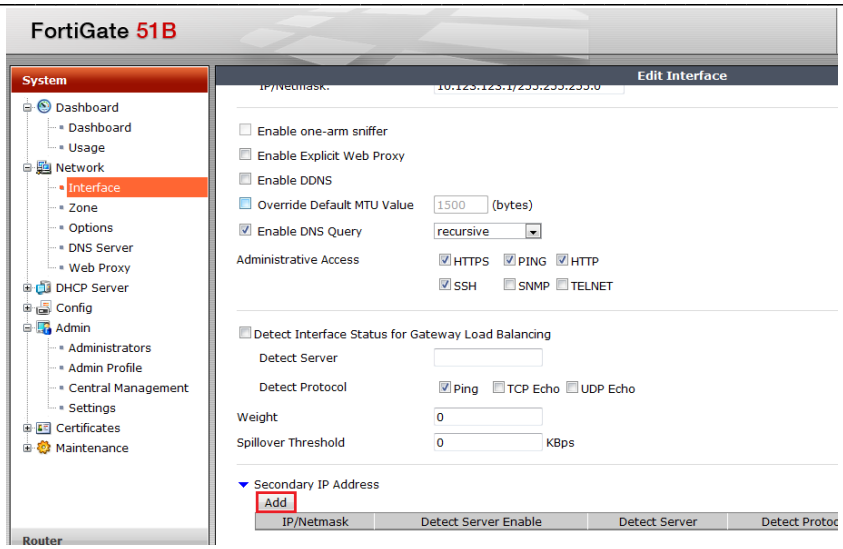

FortiGate 51B
Help
Logout
FORTINET
System
Dashboard
Dashboard
Usage
Network
Interface
Zone
Options
DNS Server
Web Proxy
Create New
Edit
Delete
[Column Settings
Name
IP/Netmask
Access
Administrative Status
Link Status
internal
10.123.123.1 / 255.255.255.0
HTTP,HTTPS,PING,SSH
wan1
200.202.114.250 / 255.255.255.248
HTTP,HTTPS,PING,SSH
wan2
0.0.0.0 / 0.0.0.0
PING

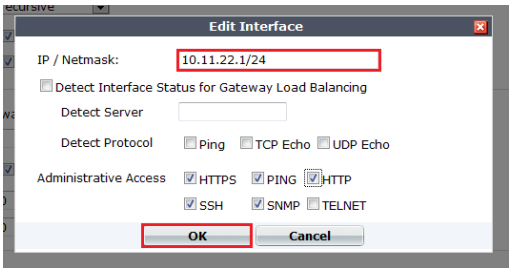

FortiGate 51B
Help
System
Dashboard
Dashboard
Usage
Network
Interface
Zone
Options
DNS Server
Web Proxy
DHCP Server
Config
Admin
Certificates
Maintenance
Router
Firewall
UTM
VPN
User
WAN Opt. & Cache
Endpoint
Log&Report
New Interface
Name
wan2_vlan100
Type
VLAN
Interface
wan2
VLAN ID
100
Addressing mode
Manual
DHCP
PPPoE
IP/Netmask:
10.1.1.1/28
Enable Explicit Web Proxy
Enable DDNS
Enable DNS Query
[Please Select]
Administrative Access
HTTPS
PING
HTTP
SSH
SNMP
TELNET
Detect Interface Status for Gateway Load Balancing
Detect Server
Detect Protocol
Ping
TCP Echo
UDP Echo
Weight
0
Spillover Threshold
0
KBps
Secondary IP Address
Description (63 characters)
OK
Cancel
Apply

***Observação**: Em equipamentos como o Fortigate-51B a Interface lógica "Internal" refere-se ao switch ao qual pertencem as portas físicas 1, 2 e 3. Desta forma, quando a interface "Internal" é configurada com VLAN, cada uma das portas físicas do switch (portas 1, 2 e 3) também serão configuradas com as VLANs em questão.

5.6.2 Endereços Secundários







Secondary IP Address

Add

IP/Netmask	Detect Server Enable	Detect Server	Detect Protocol	Administrative Access	
10.11.22.1/24	disable			https ping http ssh snmp	
10.11.44.1/24	disable			https ping http ssh snmp	
10.11.88.1/24	disable			https ping http ssh snmp	

5.6.3 Forçar Velocidade e Modo de Operação

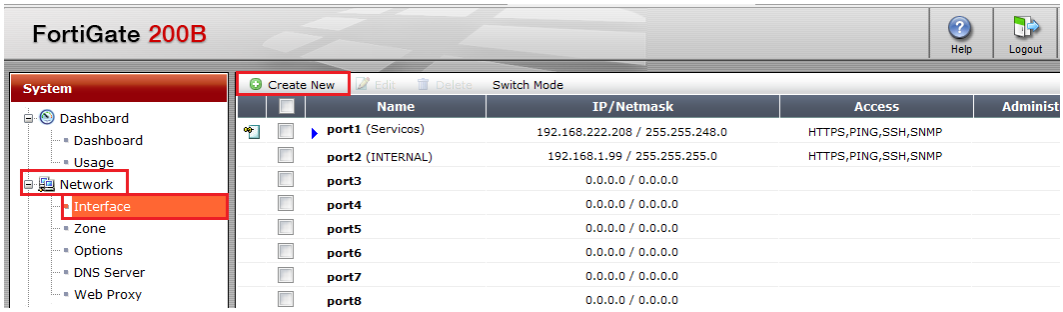
Não existe um opção opção para forçar o modo de operação de uma interface através da interface web. Isto deve ser configurado através da CLI:

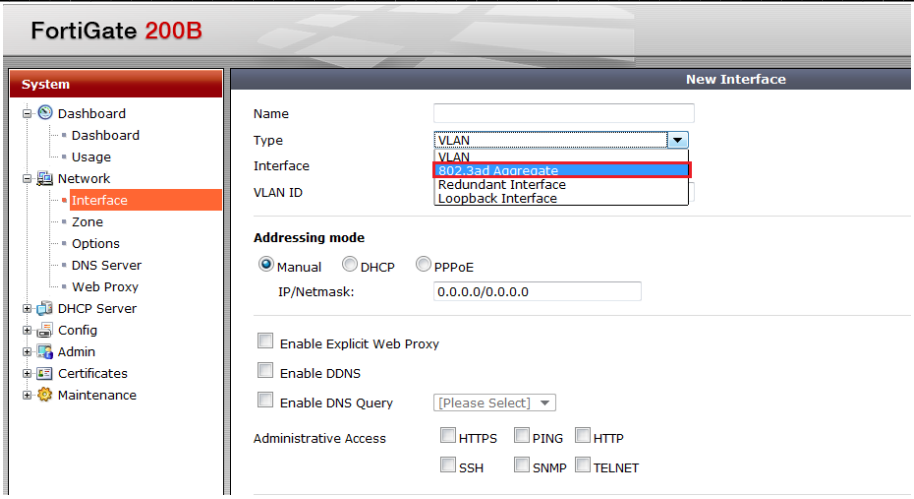
```
Fortigate51B # config system interface
Fortigate51B (interface) # edit wan1
Fortigate51B (wan1) # set speed 100full
Fortigate51B (wan1) # end
```

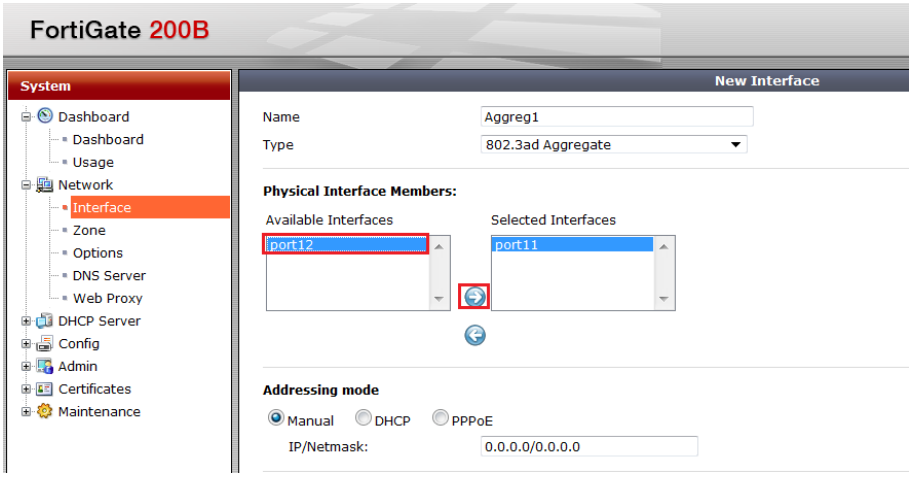
5.6.4 Verificar Modo de Operação das Interfaces

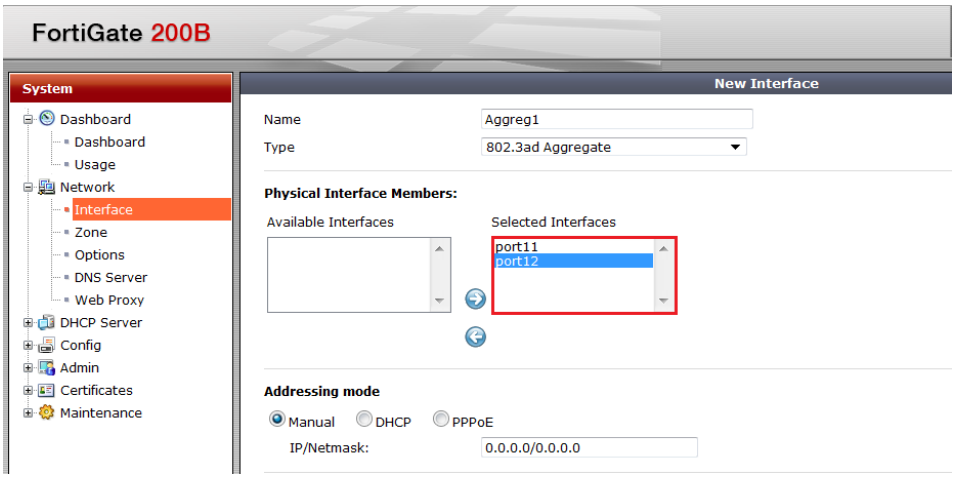
```
Fortigate51B # get system interface physical
== [onboard]
      ==[internal]
            mode: static
            ip: 10.123.123.1 255.255.255.0
            ipv6: ::/0
            status: up
            speed: 100Mbps (Duplex: full)
      ==[wan1]
            mode: static
            ip: 200.202.114.250 255.255.255.248
            ipv6: ::/0
            status: up
            speed: 100Mbps (Duplex: full)
      ==[wan2]
            mode: static
            ip: 0.0.0.0 0.0.0.0
            ipv6: ::/0
            status: down
            speed: n/a
      ==[modem]
            mode: static
            ip: 0.0.0.0 0.0.0.0
            ipv6: ::/0
            status: down
            speed: n/a
```

5.6.5 Agregação de Portas – 802.3AD



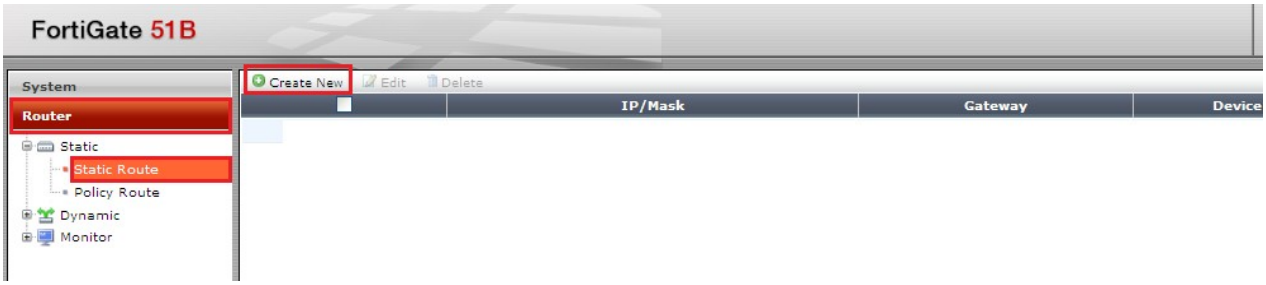

FortiGate 200B
System
Dashboard
Dashboard
Usage
Network
Interface
Zone
Options
DNS Server
Web Proxy
DHCP Server
Config
Admin
Certificates
Maintenance
New Interface
Name
Type
VLAN
Interface
VLAN ID
VLAN
802.3ad Aggregate
Redundant Interface
Loopback Interface
Addressing mode
Manual
DHCP
PPPoE
IP/Netmask:
0.0.0.0/0.0.0.0
Enable Explicit Web Proxy
Enable DDNS
Enable DNS Query
[Please Select]
Administrative Access
HTTPS
PING
HTTP
SSH
SNMP
TELNET

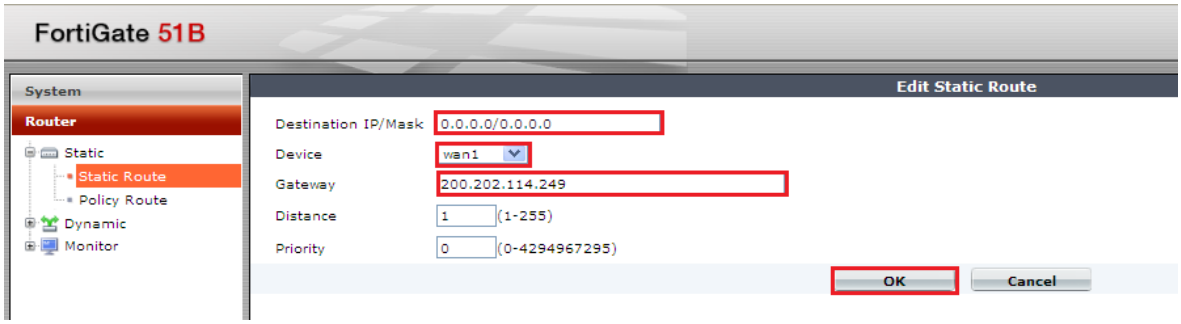

FortiGate 200B
System
Dashboard
Dashboard
Usage
Network
Interface
Zone
Options
DNS Server
Web Proxy
DHCP Server
Config
Admin
Certificates
Maintenance
New Interface
Name
Aggreg1
Type
802.3ad Aggregate
Physical Interface Members:
Available Interfaces
Selected Interfaces
port12
port11
Addressing mode
Manual
DHCP
PPPoE
IP/Netmask:
0.0.0.0/0.0.0.0

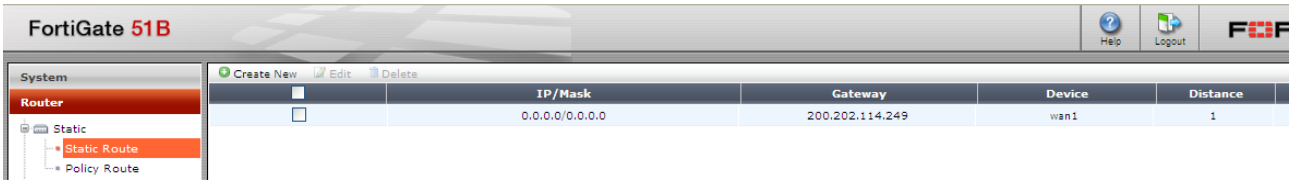

FortiGate 200B
System
Dashboard
Dashboard
Usage
Network
Interface
Zone
Options
DNS Server
Web Proxy
DHCP Server
Config
Admin
Certificates
Maintenance
New Interface
Name
Aggreg1
Type
802.3ad Aggregate
Physical Interface Members:
Available Interfaces
Selected Interfaces
port11
port12
Addressing mode
Manual
DHCP
PPPoE
IP/Netmask:
0.0.0.0/0.0.0.0

5.7 Rotas

As configurações de rotas são realizadas em Router -> Static ->Static Route





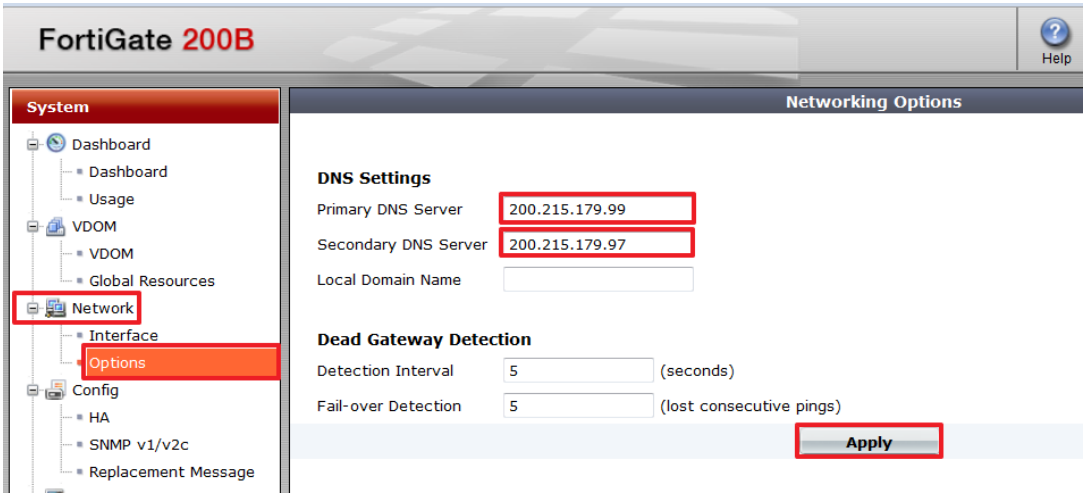


A configuração de uma rota default é exemplificada através dos comandos abaixo:

```
Fortigate51B # config router static
Fortigate51B #edit 1
Fortigate51B (1) # set device "wan1"
Fortigate51B (1) # set gateway 200.202.114.249
Fortigate51B (1) # end
```

5.8 DNS

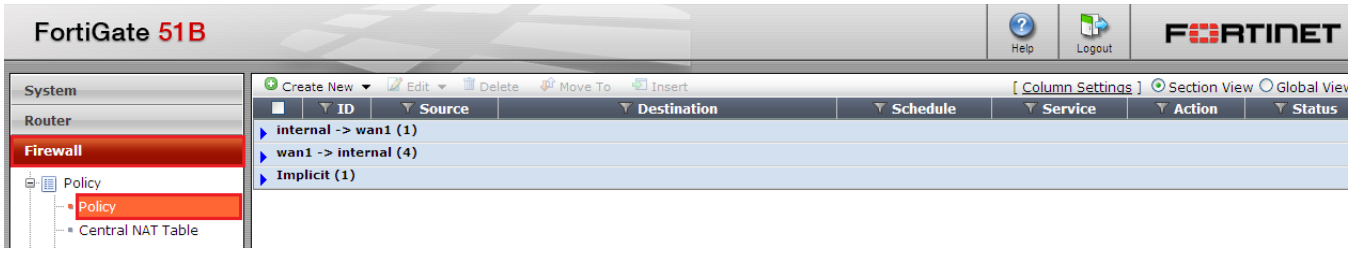
Alguns serviços (ex: atualização de assinatura do IPS) podem exigir que o FortiGate execute a resolução de nomes. Pode-se configurar DNSs através de System -> Network -> Options



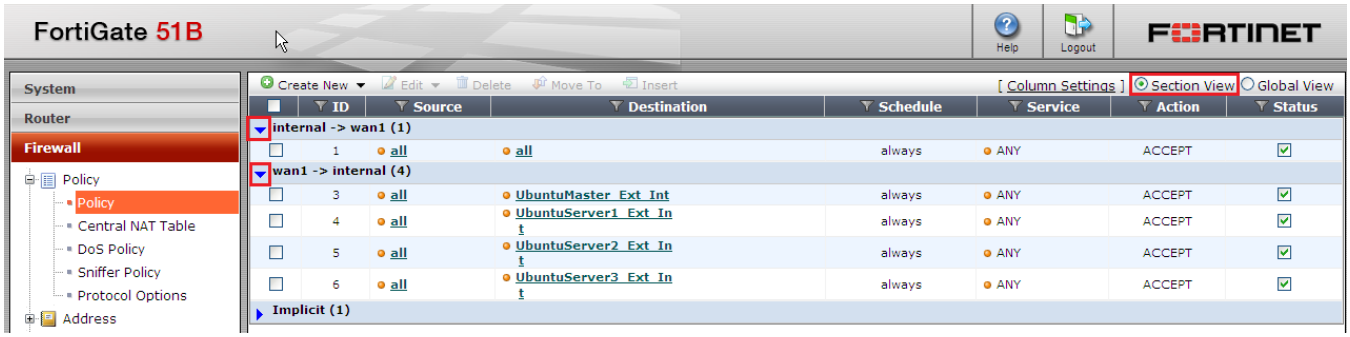
6 Firewall

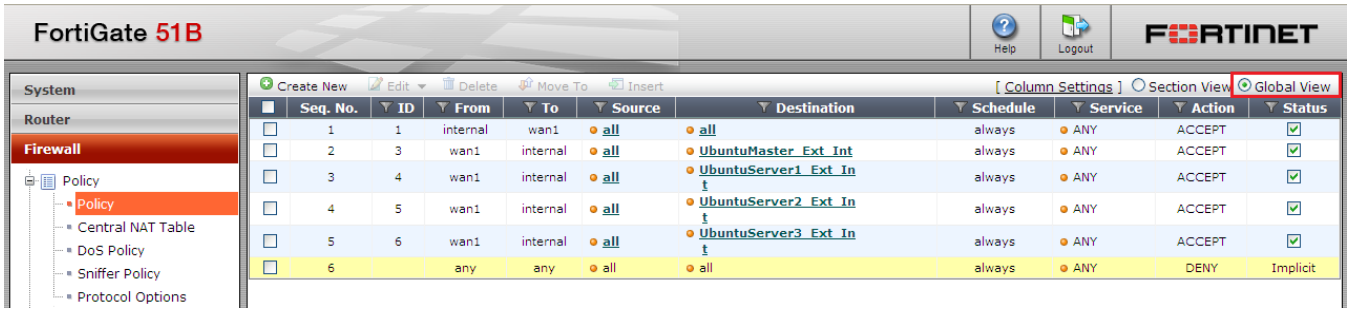
6.1 Regras

As regras podem ser configuradas em Firewall-> Policy -> Policy.



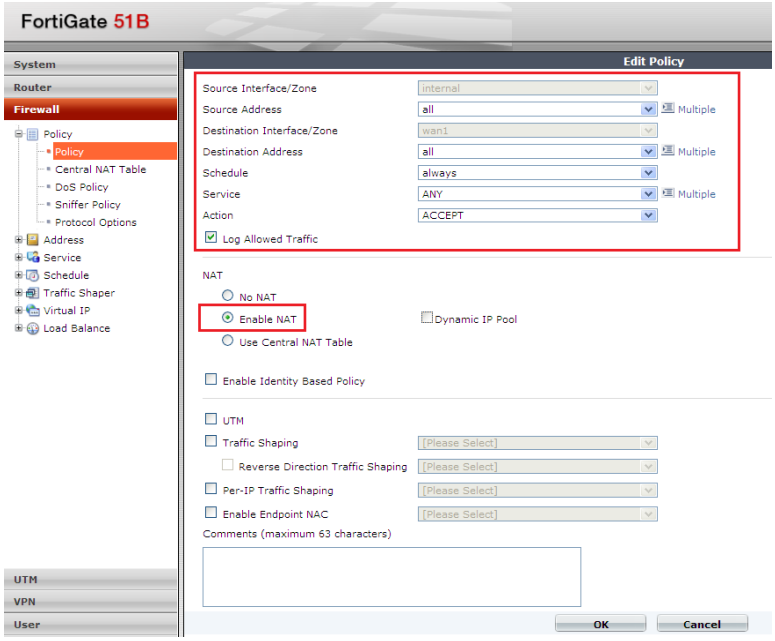
Section View





6.1.1 Regra Default

Por default o Fortigate realiza o NAT dos acessos internos para o endereço externo da WAN1 do firewall:

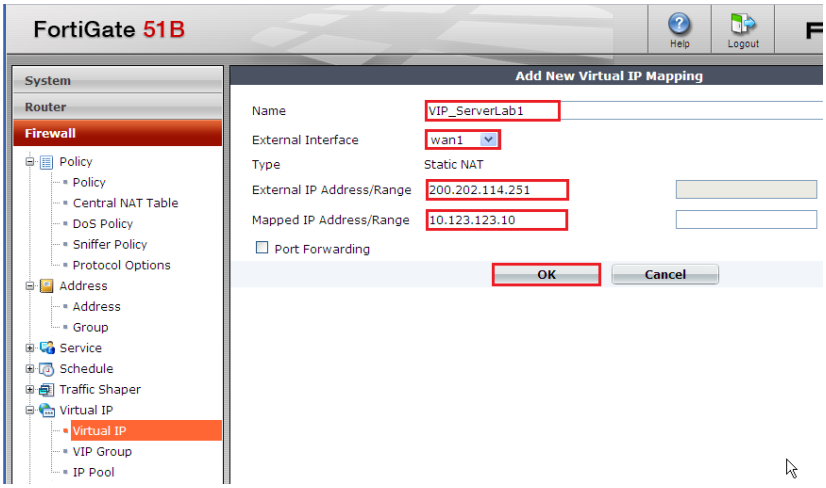


6.2 NAT

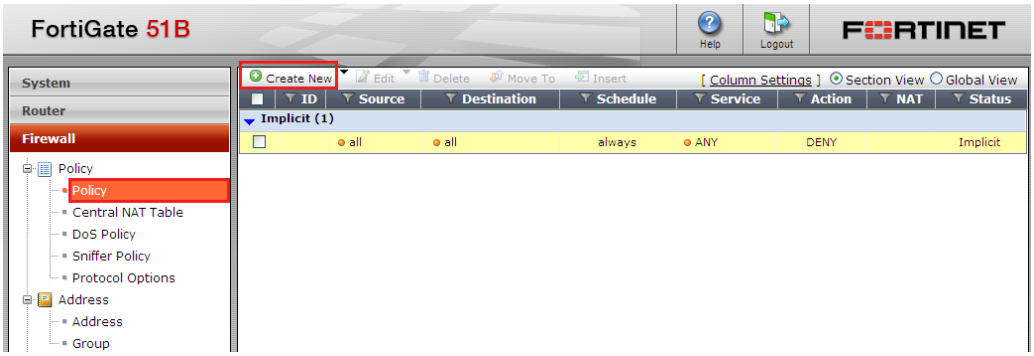
6.2.1 Exemplo 1 – Virtual IP (VIP) - NAT de Entrada

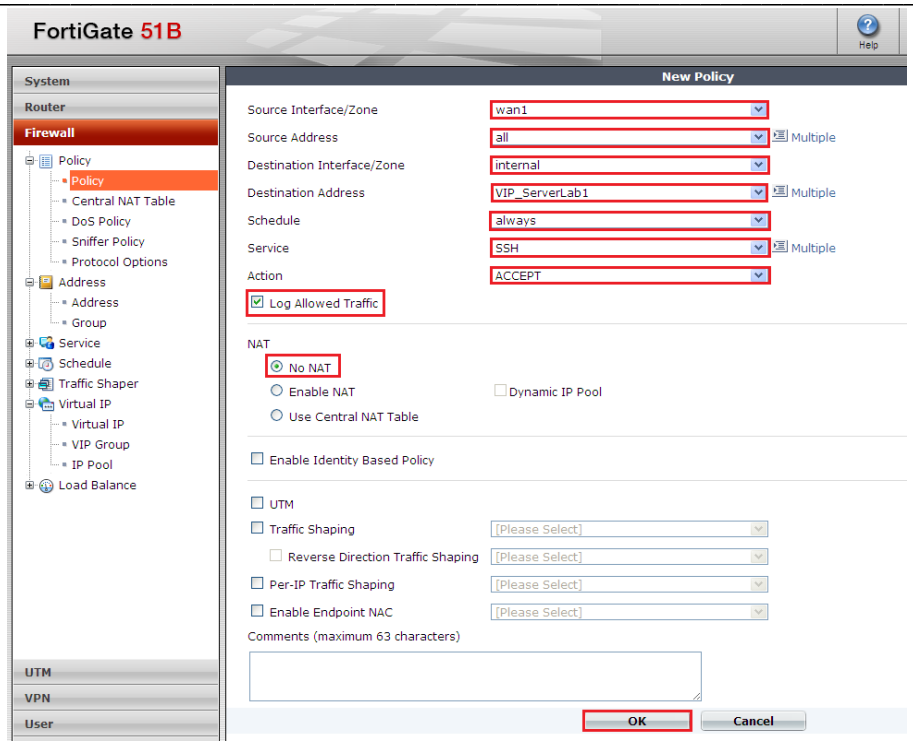
Endereço Interno: 10.123.123.10
Endereço Externo: 200.202.114.251

1. Criar Virtual IP



2. Criar regra de entrada





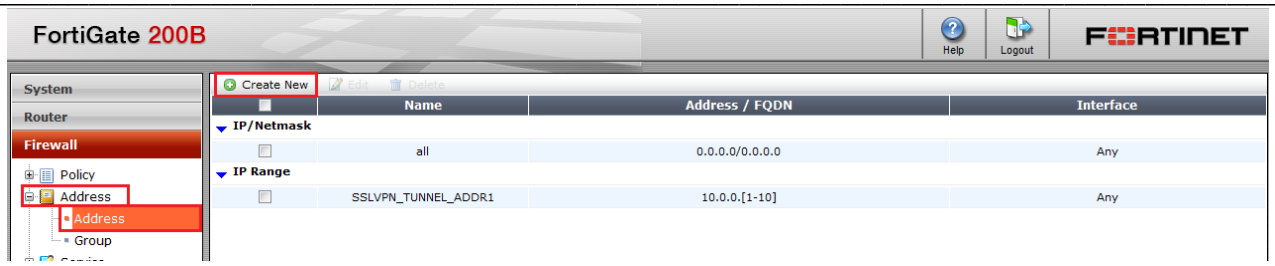
*Obs: Mesmo sem habilitar o NAT na regra, o NAT será realizado pois foi definido no Virtual IP.

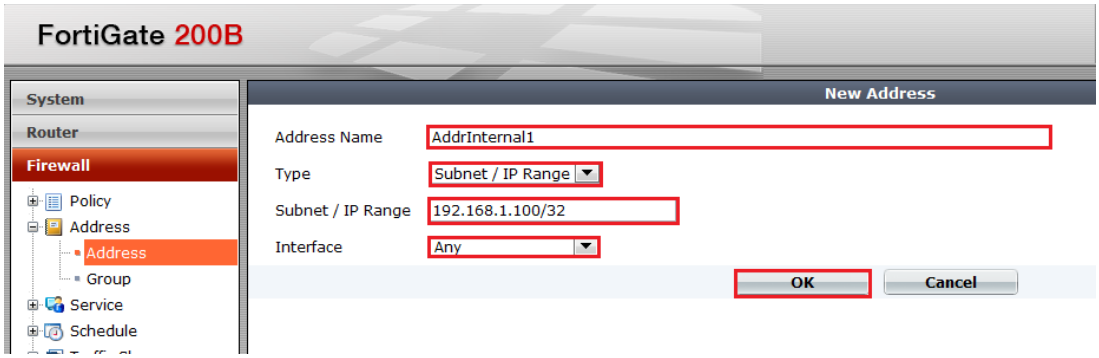
6.2.2 Exemplo 2 – IP Pool – NAT de Saída

Este exemplo apresenta um configuração de NAT de saída (source NAT) com tradução 1 para 1, usando o método de IP Pool.

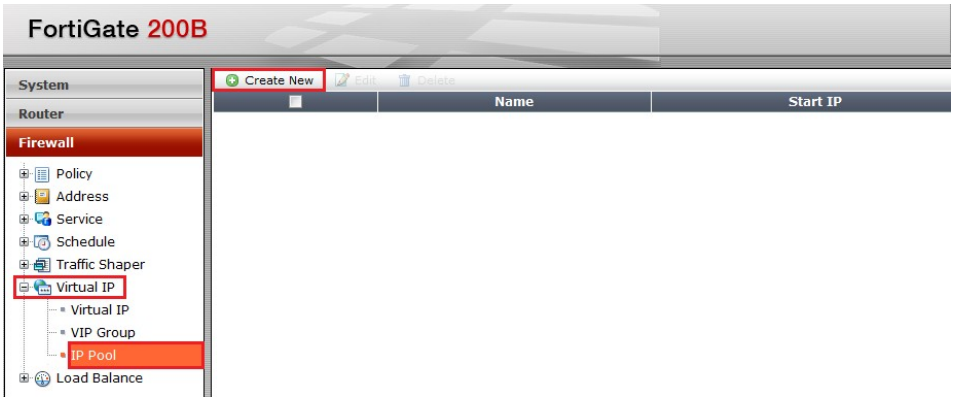
Neste exemplo o endereço interno 192.168.1.100 será traduzido para 200.189.190.108 quando for encaminhado para a Internet.

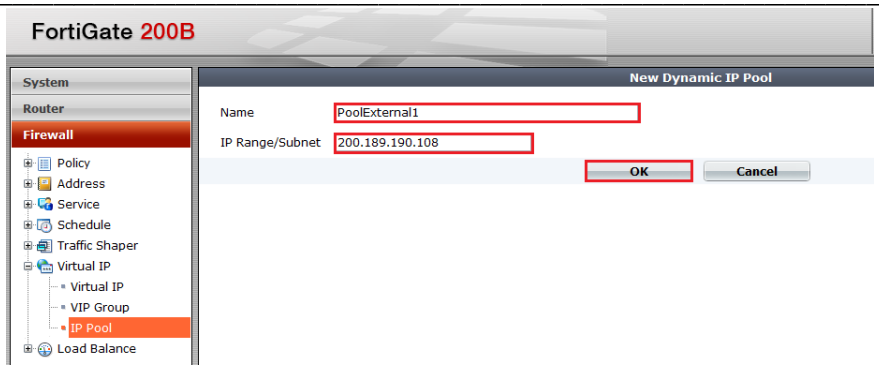
1. Criar endereço interno



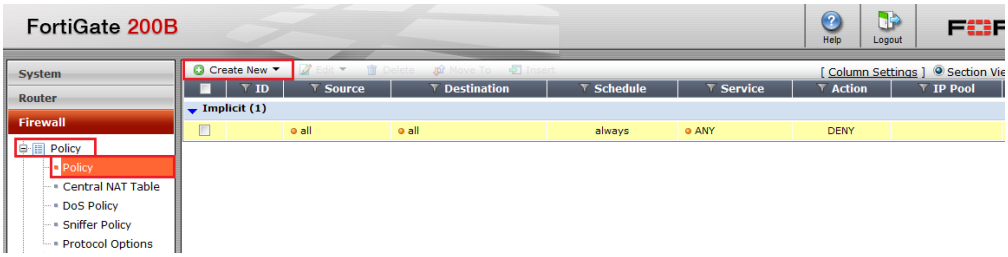


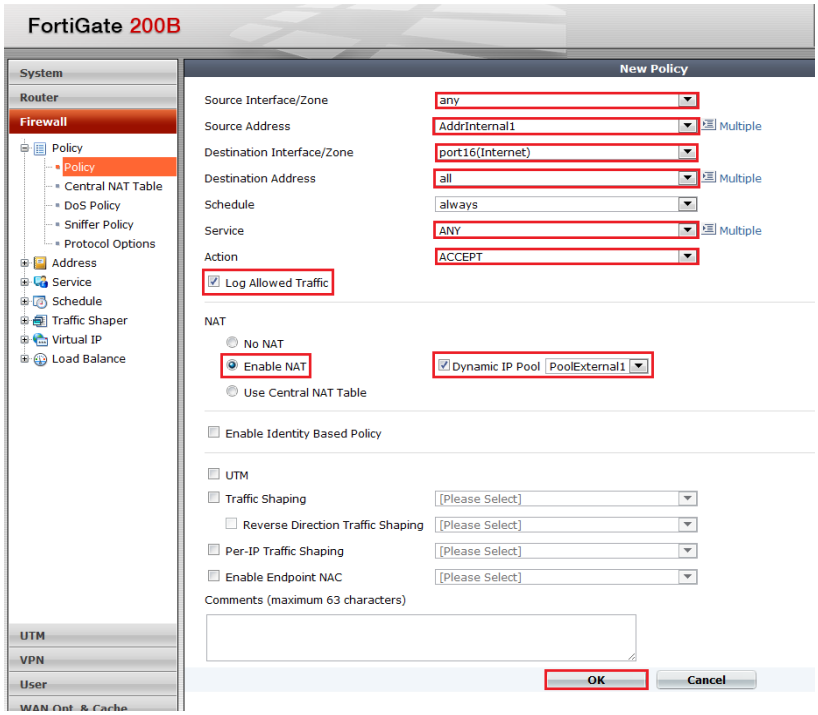
2. Criar IP Pool com o endereço externo

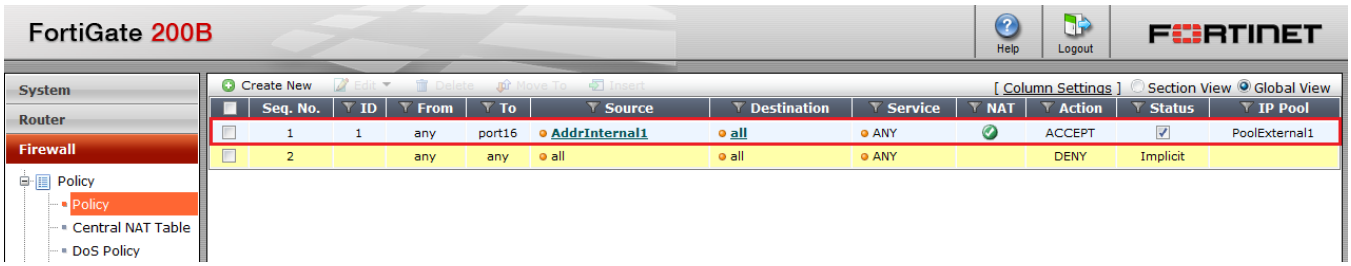




3. Criar regra de saída



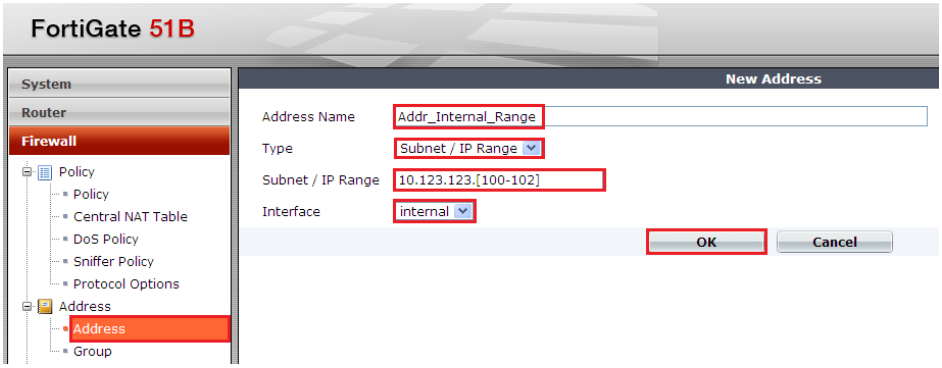




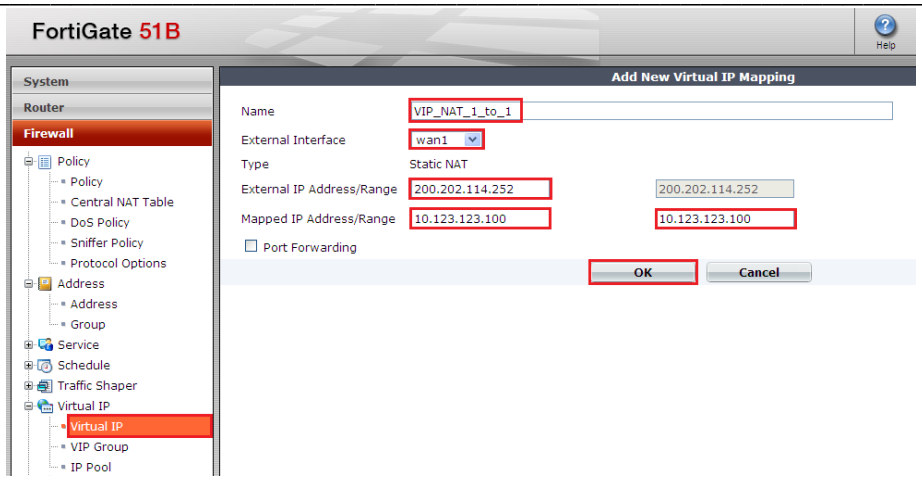
6.2.3 Exemplo 3 - Virtual IP (VIP) - NAT de Saída

Este exemplo apresenta um configuração de NAT de saída (source NAT) com tradução 1 para 1, usando o método de Virtual IPs.

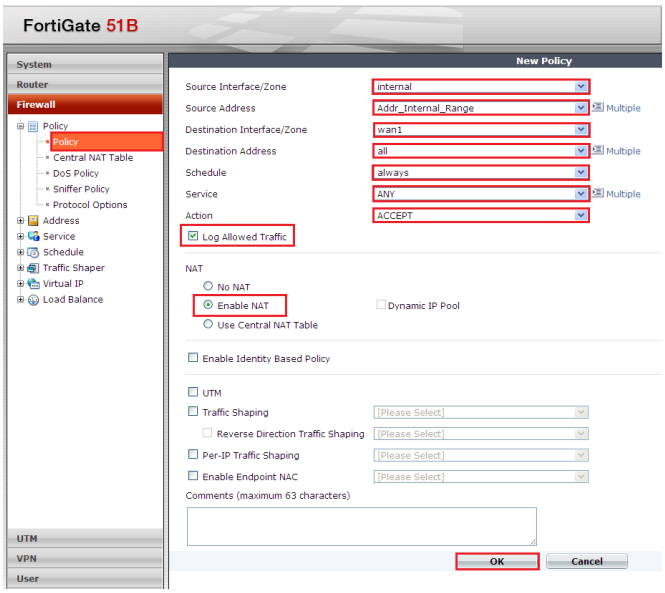
1. Criar Endereço do Range Interno



2. Criar Virtual IP do Range Externo



3. Criar Regra de Saída – Usar o Endereço do Range Interno no Source.

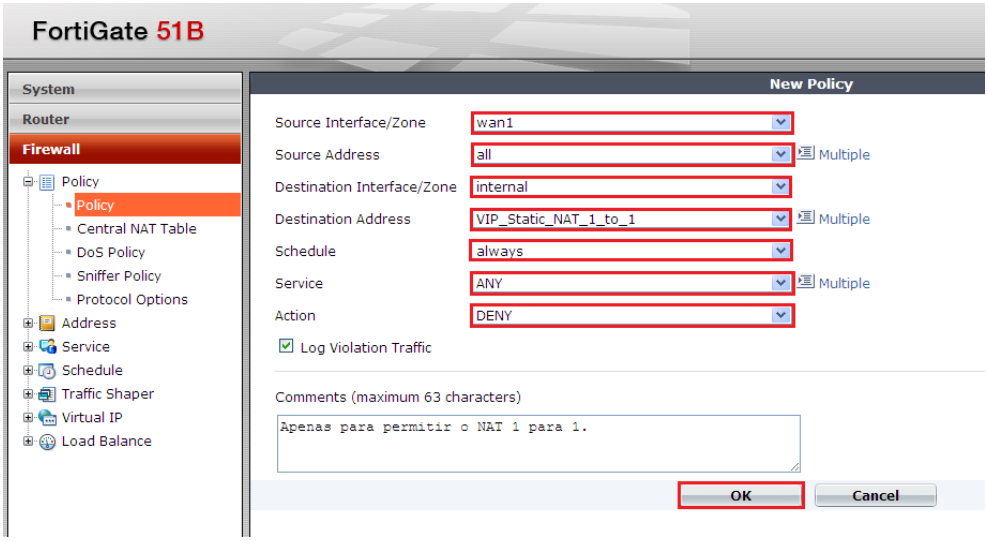


4. Criar Regra de Entrada – Usar o Virtual IP do Range Externo

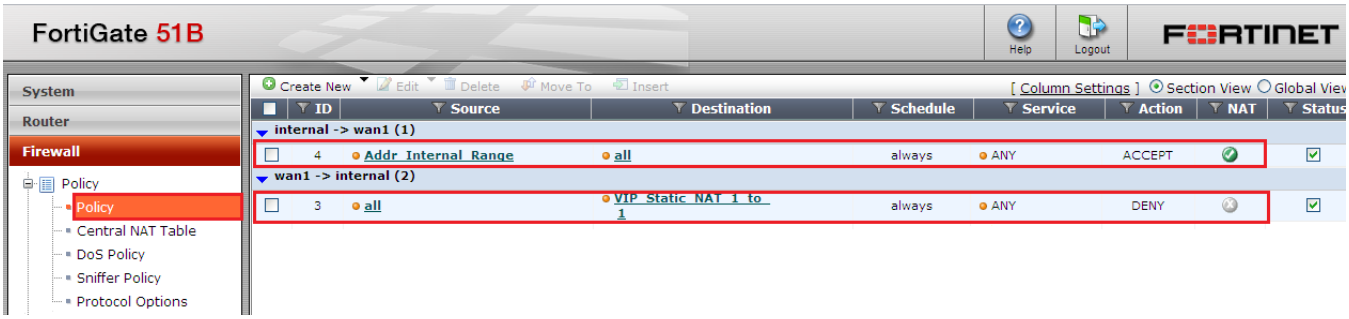
Obs:** ***É necessário criar uma regra de entrada mesmo que não exista a necessidade de acessos do ambiente externo para o interno. Esta regra

é necessária para que o NAT funcione corretamente. Ver página 124 do manual Fortigate Fundamentals – FortiOS Handbook 4.0 MR2 - "Using VIP range for Source NAT (SNAT) and Static 1-to-1 mapping".

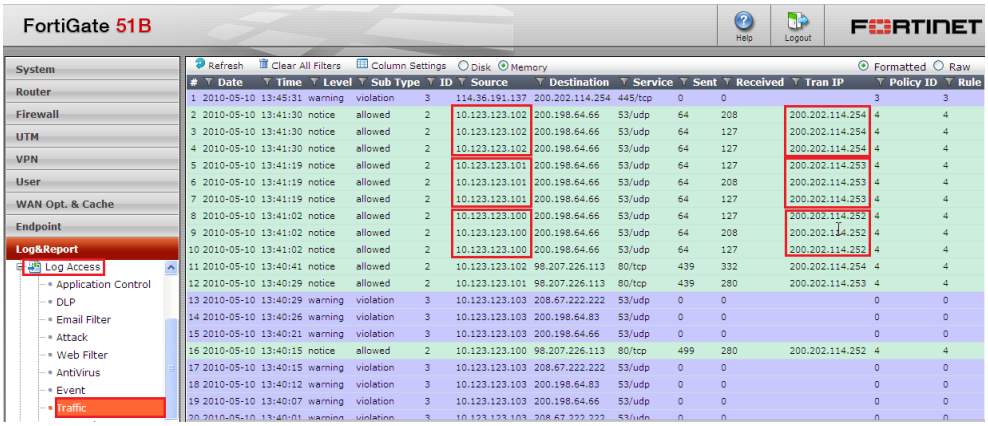
O exemplo a seguir apresenta uma configuração em que não há a necessidade de acessos do ambiente externo para o interno. Neste caso deve-se então criar uma regra de entrada onde o Action é DENY.



5. Configuração Final:

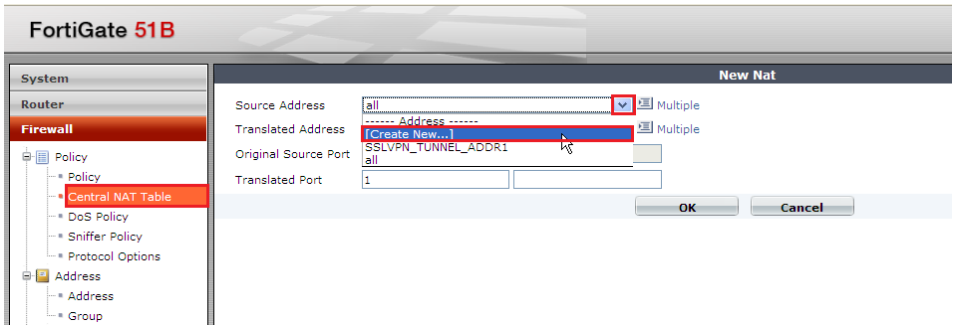


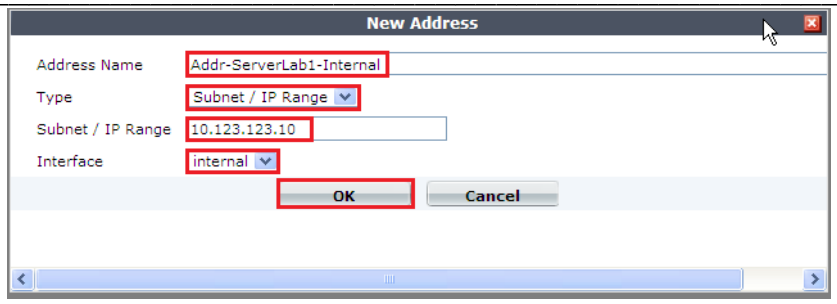
6. Verificação do NAT no Log

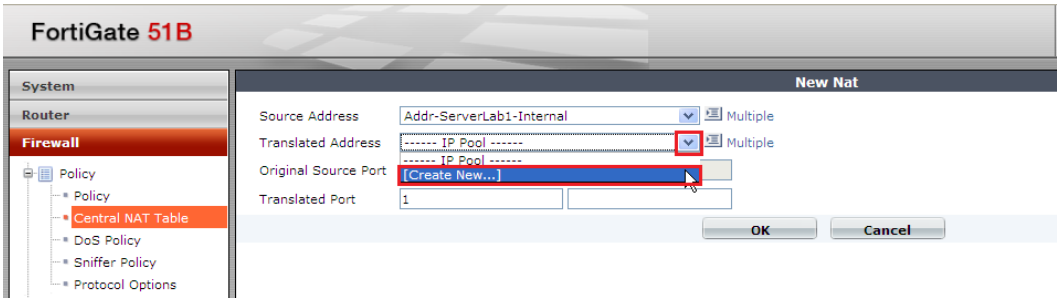


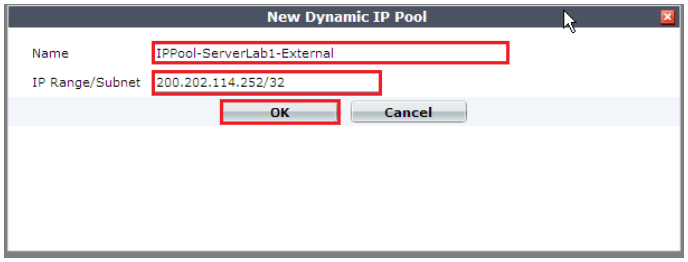
6.2.4 Exemplo 4 - Central NAT Table - NAT de Saída

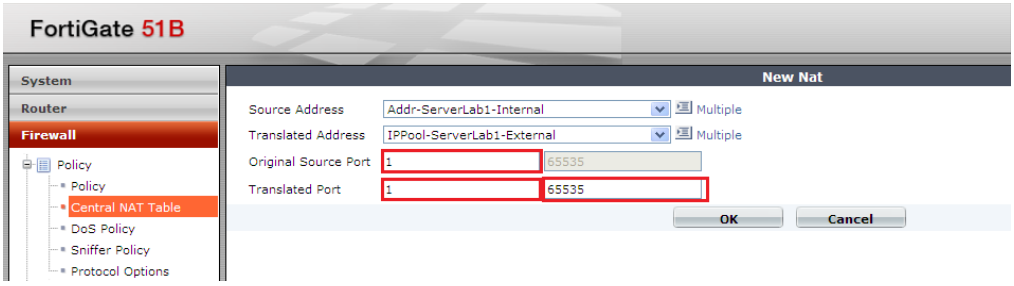
Este exemplo apresenta um configuração de NAT de saída (source NAT) com tradução 1 para 1, usando o método de Central NAT Table para as traduções de saída. Para as traduções de entrada será usado o método de Virtual IP.



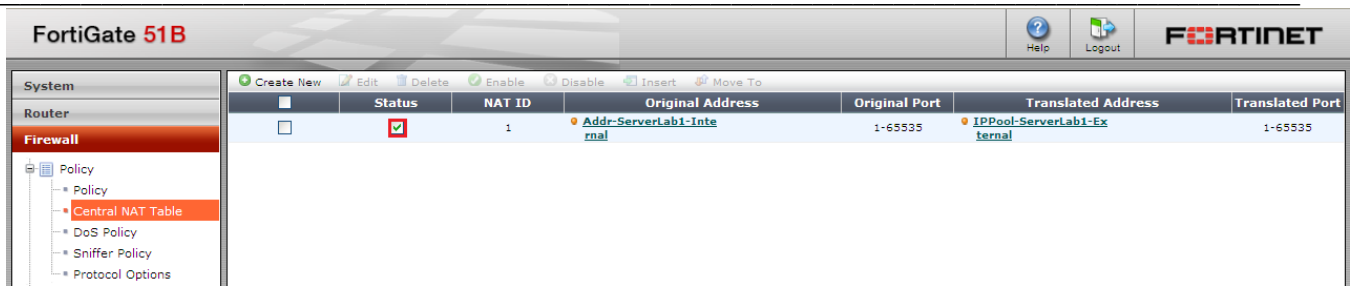


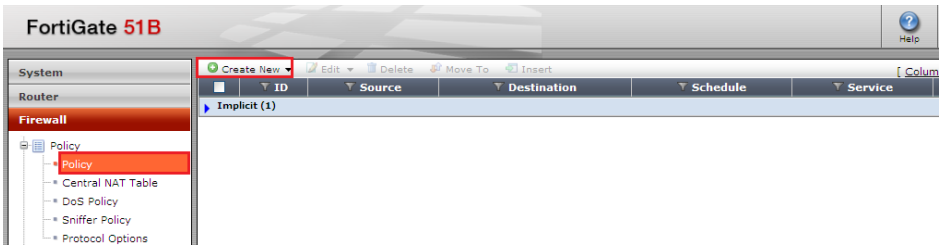


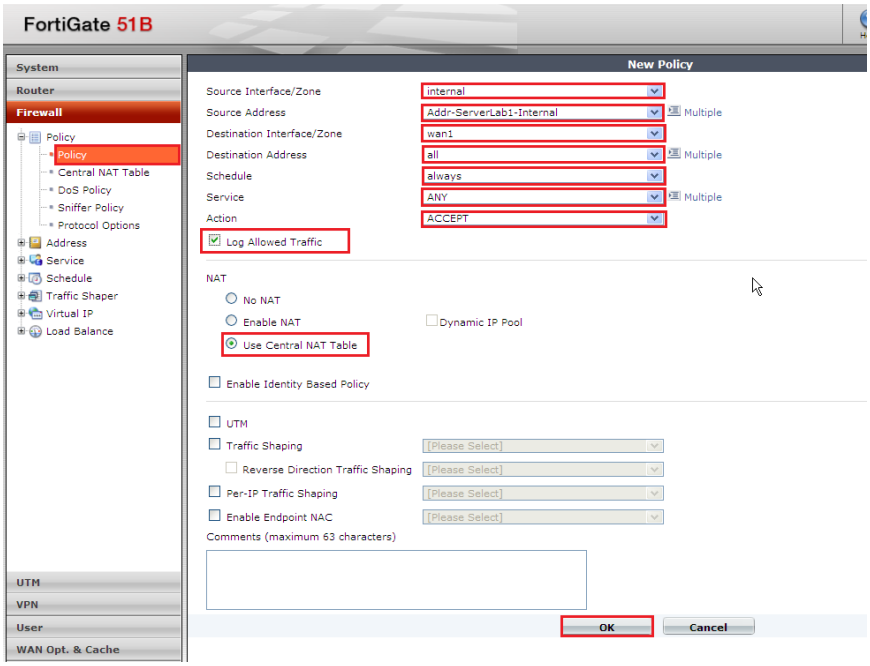




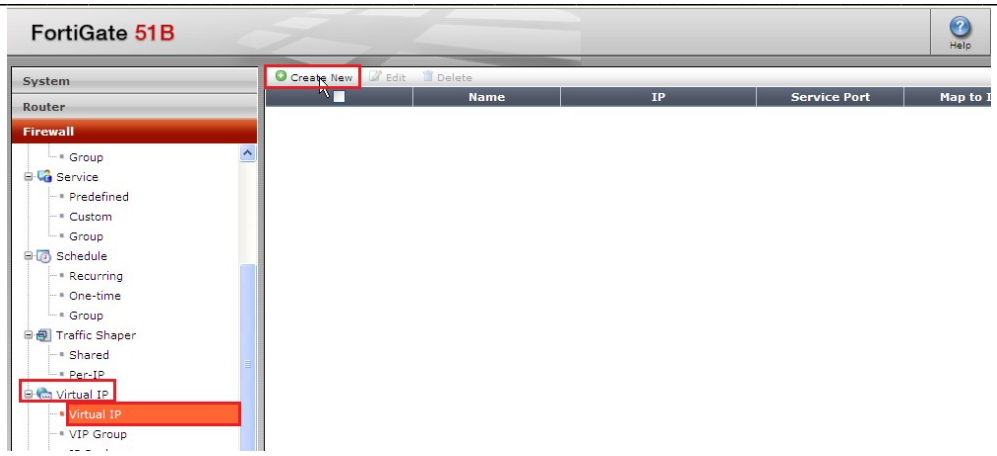
Verificar a regra de NAT criada na Central NAT Table e se o seu status está enabled:

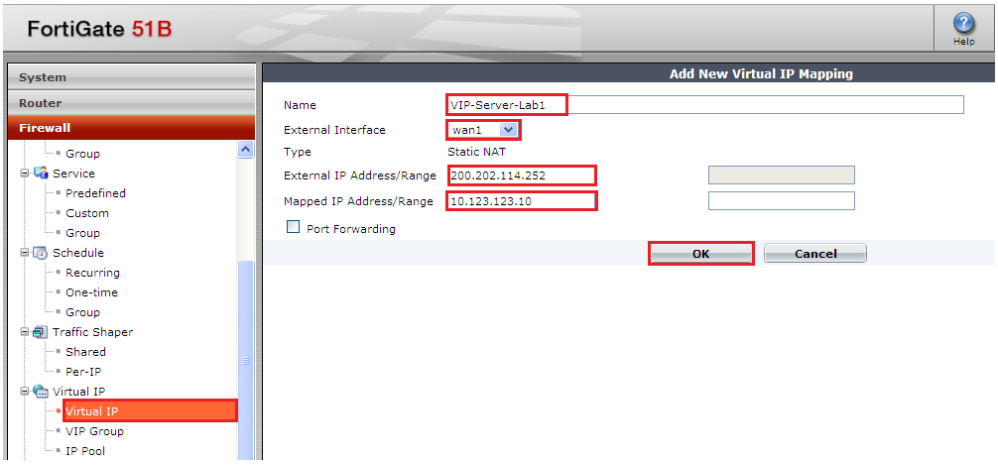


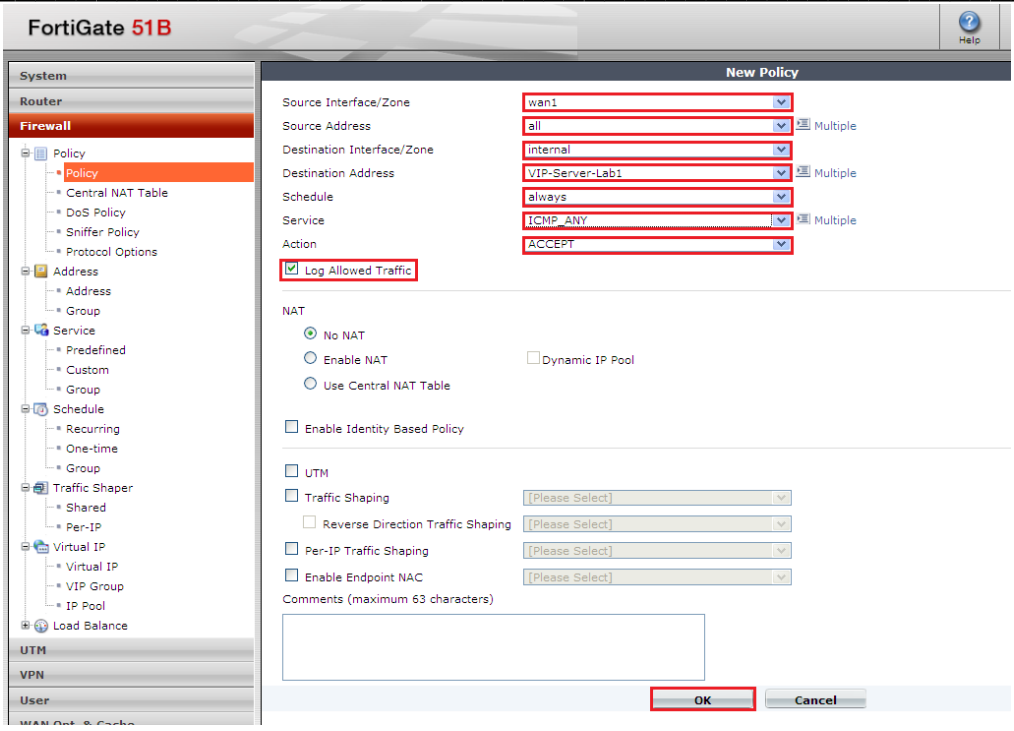


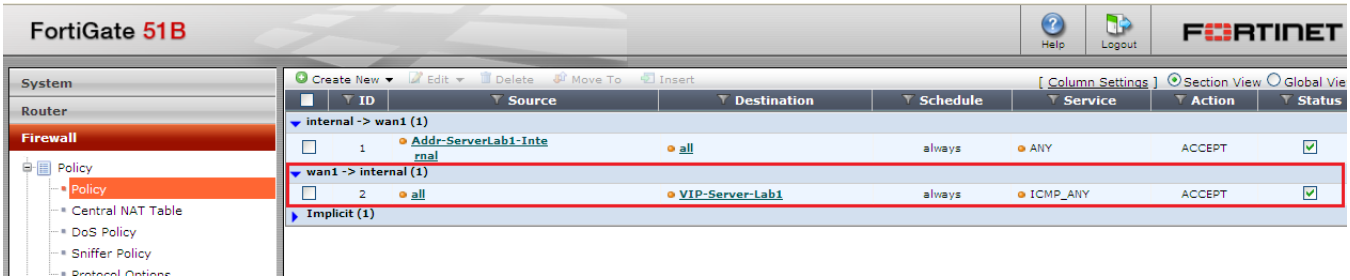


Supondo que este equipamento receberá conexões provenientes da Internet deve-se fazer um NAT de entrada. O NAT de entrada é realizado através de um Virtual IP.

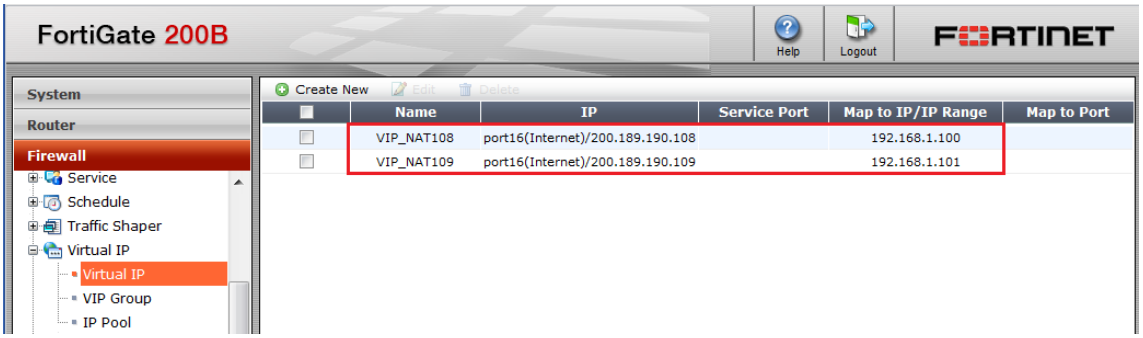

FortiGate 51B
Help
System
Router
Firewall
Group
Service
Predefined
Custom
Group
Schedule
Recurring
One-time
Group
Traffic Shaper
Shared
Per-IP
Virtual IP
Virtual IP
VIP Group
Create New
Edit
Delete
Name
IP
Service Port

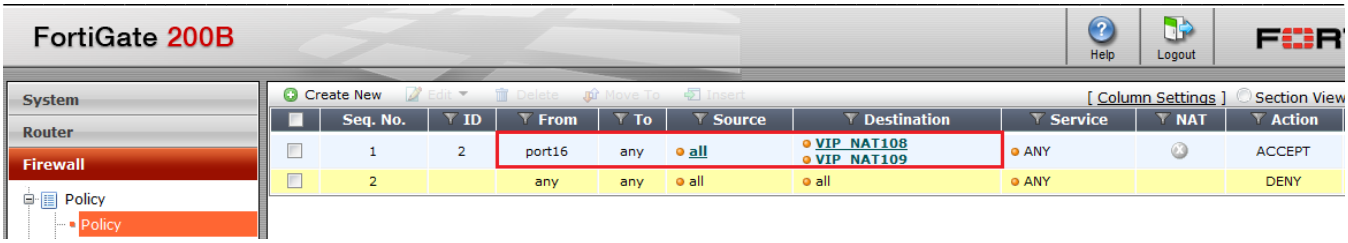

FortiGate 51B
Help
System
Router
Firewall
Group
Service
Predefined
Custom
Group
Schedule
Recurring
One-time
Group
Traffic Shaper
Shared
Per-IP
Virtual IP
Virtual IP
VIP Group
IP Pool
Add New Virtual IP Mapping
Name
VIP-Server-Lab1
External Interface
wan1
Type
Static NAT
External IP Address/Range
200.202.114.252
Mapped IP Address/Range
10.123.123.10
Port Forwarding
OK
Cancel





6.2.5 Exemplo 5 - Vários NAT de Entrada na Mesma Regra





6.3 Session/Service Timeout

Não é possível ajustar o time-out/TTL dos serviços através da interface web. Para tanto deve-se usa a CLI.

Verificar o TTL usado nas sessões e serviços:

```
Fortigate51B # get system session-ttl
default              : 3600
port:
```

Ajustar o TTL:

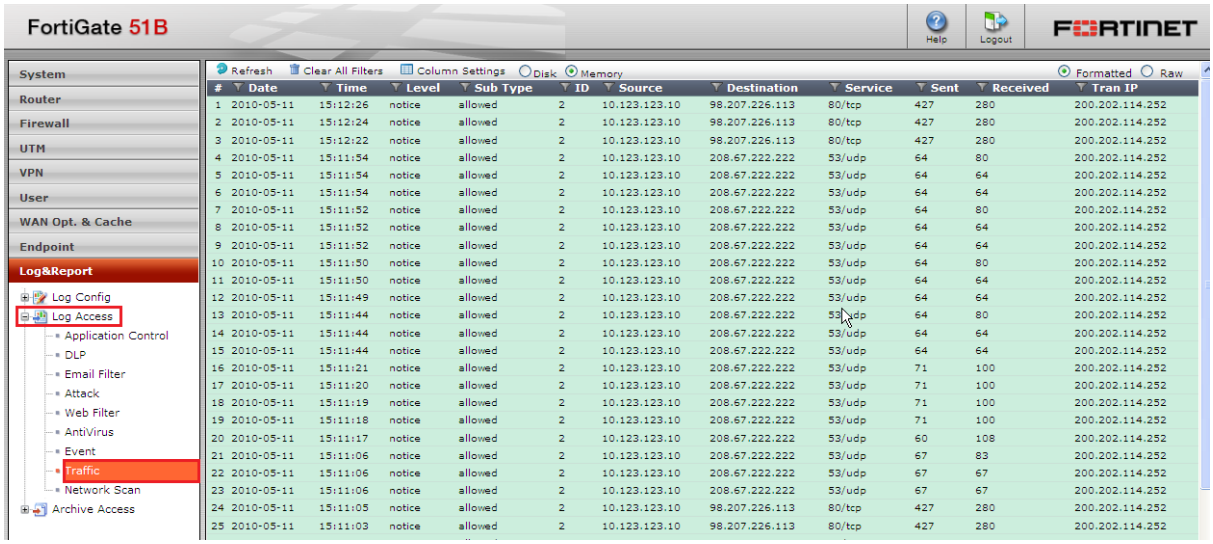
- Default para 300 segundos (todos os serviços);
- TCP/80 (HTTP) para 120 segundos;
- UDP/53 (DNS) para 60 segundos;

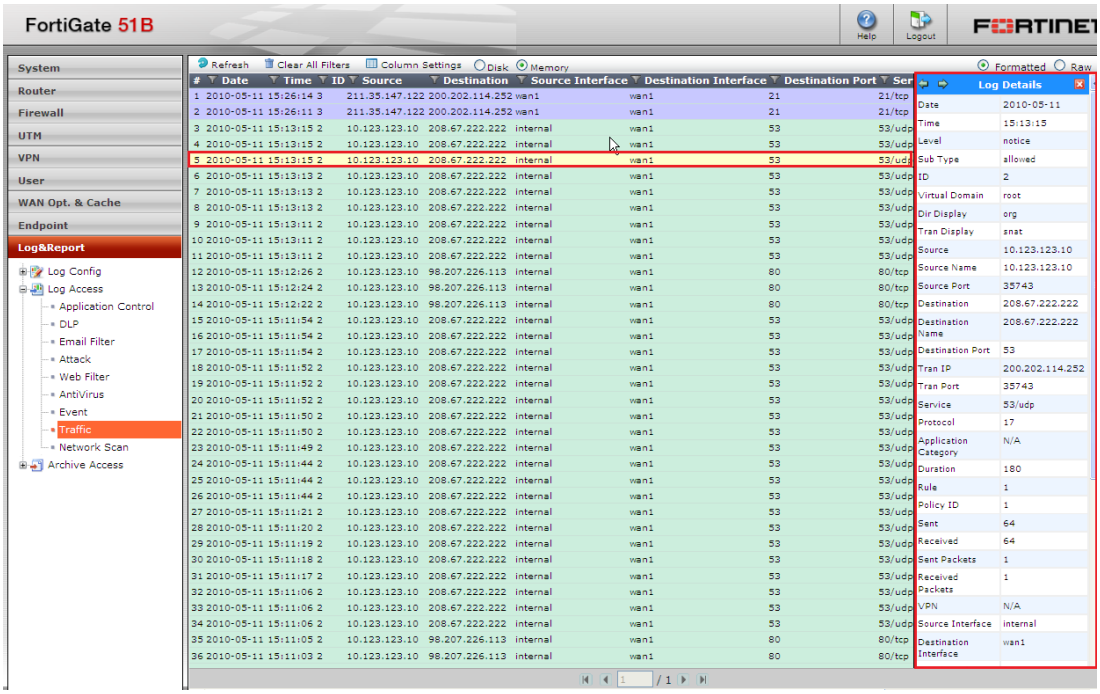
```
Fortigate51B # sh system session-ttl
config system session-ttl
    set default 300
        config port
            edit 80
                set protocol 6
                set timeout 120
                set end-port 80
                set start-port 80
            next
            edit 53
                set protocol 17
                set timeout 60
                set end-port 53
```

```
                set start-port 53
            next
        end
end
```

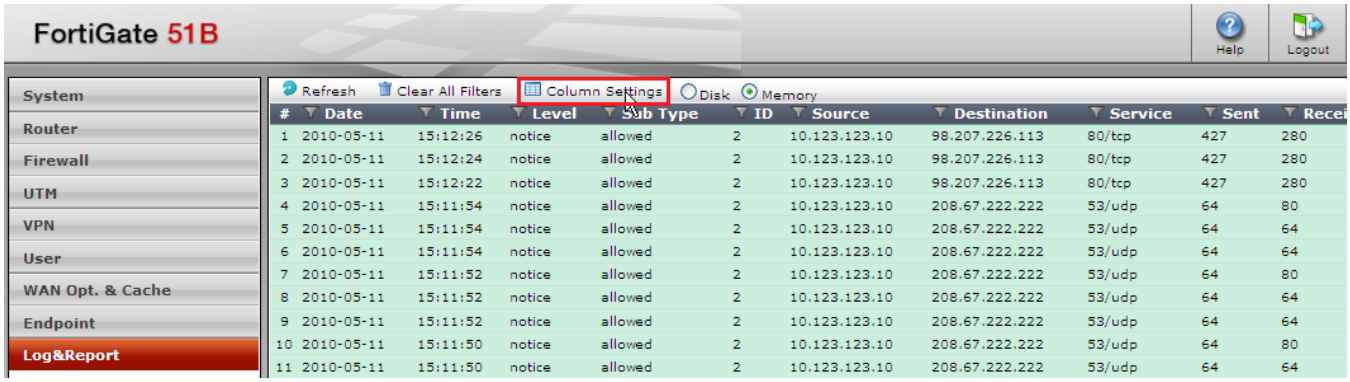
7 Log

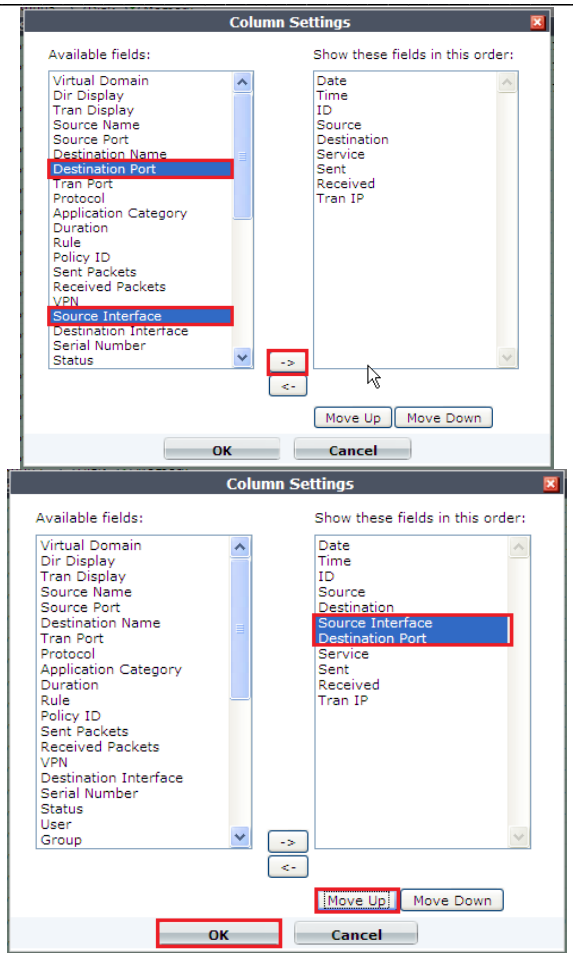
A configuração e acesso aos logs é realizado através de Log&Report;

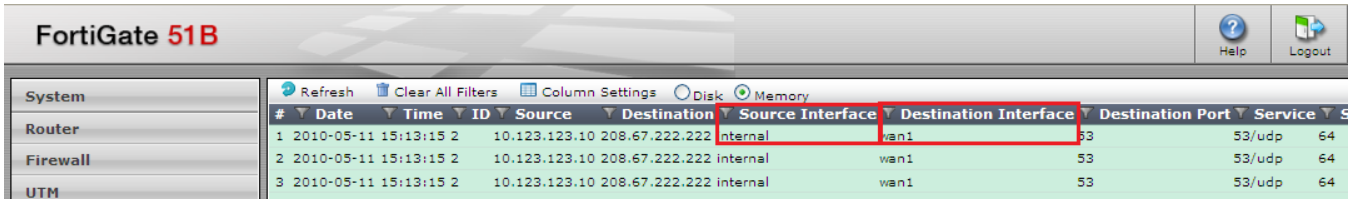




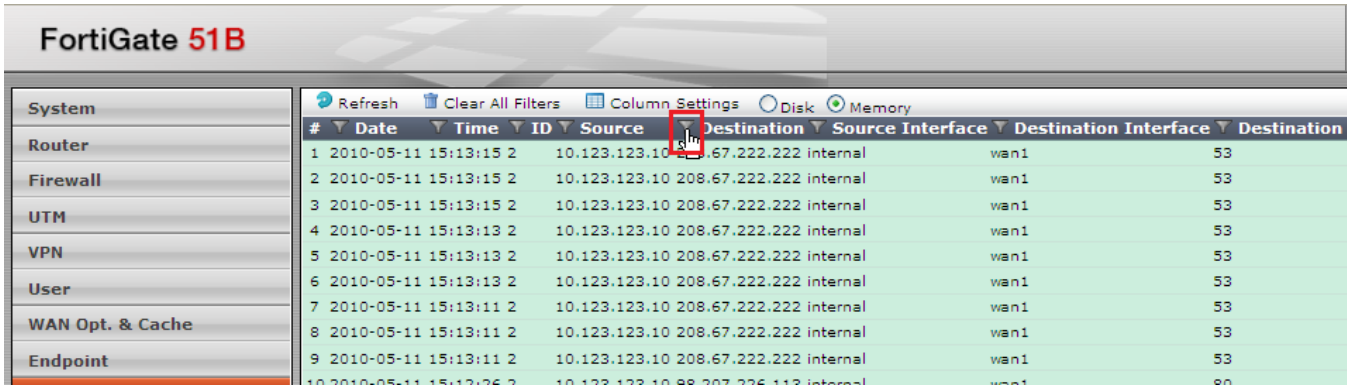
7.1 Configuração

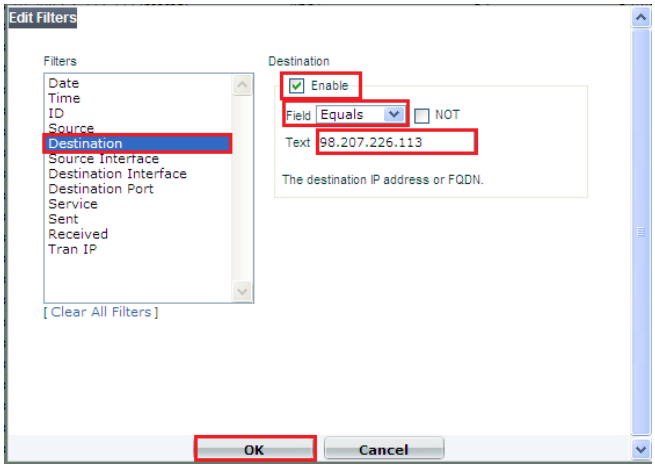


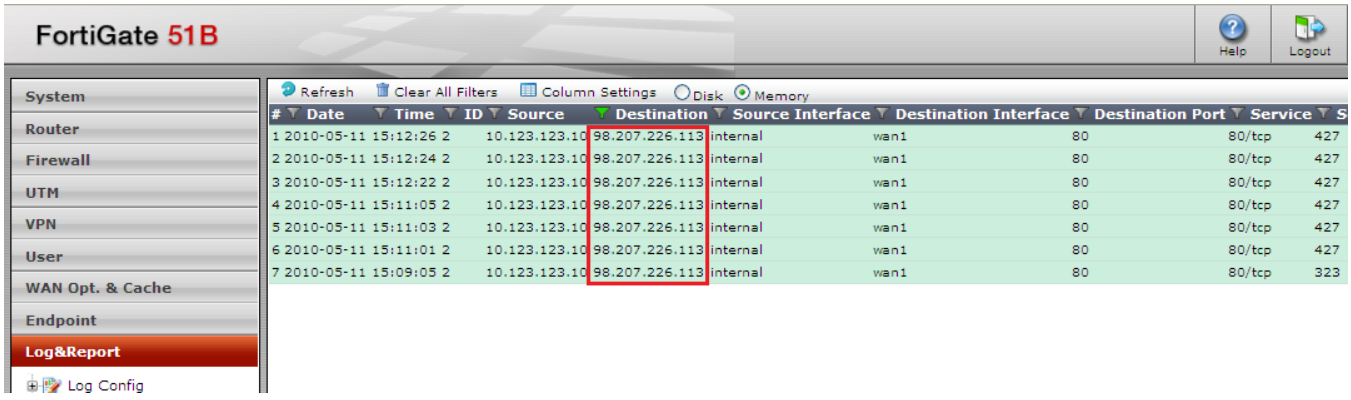

Column Settings
Available fields:
Virtual Domain
Dir Display
Tran Display
Source Name
Source Port
Destination Name
Destination Port
Tran Port
Protocol
Application Category
Duration
Rule
Policy ID
Sent Packets
Received Packets
VPN
Source Interface
Destination Interface
Serial Number
Status
Show these fields in this order:
Date
Time
ID
Source
Destination
Service
Sent
Received
Tran IP
->
<-
Move Up
Move Down
OK
Cancel
Column Settings
Available fields:
Virtual Domain
Dir Display
Tran Display
Source Name
Source Port
Destination Name
Tran Port
Protocol
Application Category
Duration
Rule
Policy ID
Sent Packets
Received Packets
VPN
Destination Interface
Serial Number
Status
User
Group
Show these fields in this order:
Date
Time
ID
Source
Destination
Source Interface
Destination Port
Service
Sent
Received
Tran IP
->
<-
Move Up
Move Down
OK
Cancel

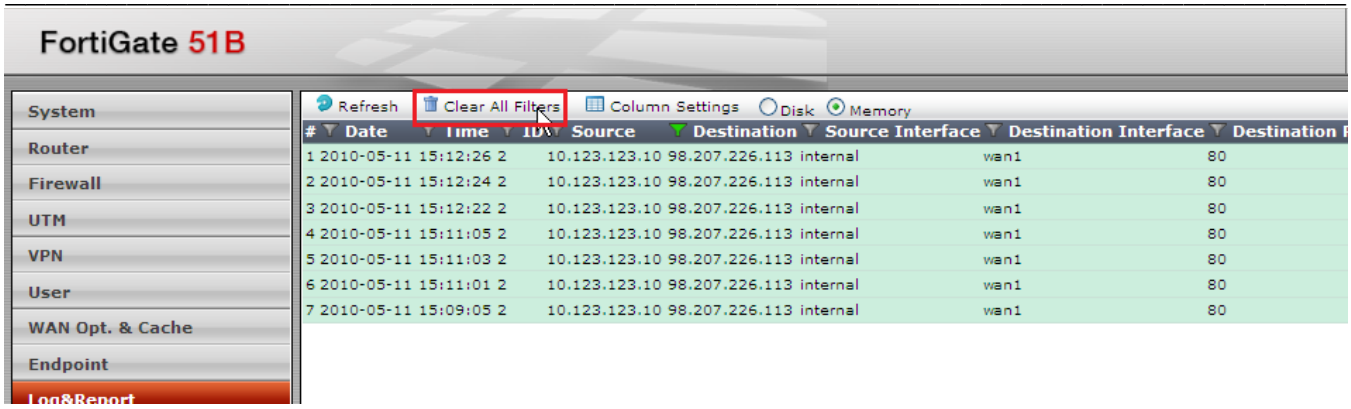

FortiGate 51B
Help
Logout
System
Router
Firewall
UTM
Refresh
Clear All Filters
Column Settings
Disk
Memory
Date Time ID Source Destination Source Interface Destination Interface Destination Port Service
1 2010-05-11 15:13:15 2 10.123.123.10 208.67.222.222 internal wan1 53 53/udp 64
2 2010-05-11 15:13:15 2 10.123.123.10 208.67.222.222 internal wan1 53 53/udp 64
3 2010-05-11 15:13:15 2 10.123.123.10 208.67.222.222 internal wan1 53 53/udp 64

7.2 Filtro

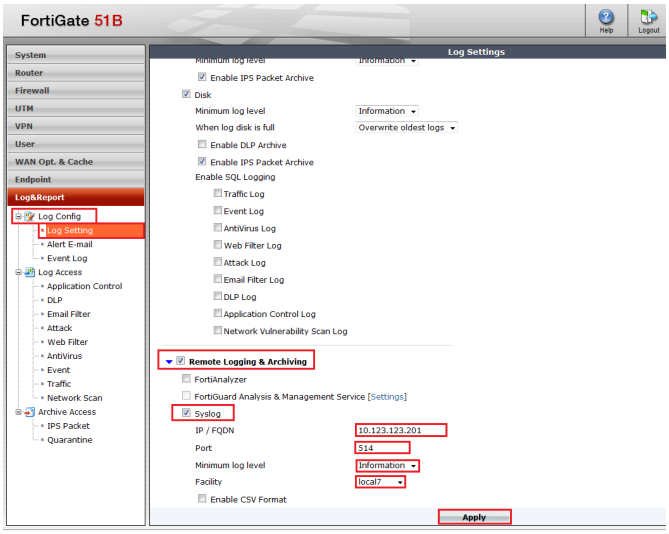

FortiGate 51B
System
Router
Firewall
UTM
VPN
User
WAN Opt. & Cache
Endpoint
Refresh
Clear All Filters
Column Settings
Disk
Memory
Date Time ID Source Destination Source Interface Destination Interface Destination
1 2010-05-11 15:13:15 2 10.123.123.10 208.67.222.222 internal wan1 53
2 2010-05-11 15:13:15 2 10.123.123.10 208.67.222.222 internal wan1 53
3 2010-05-11 15:13:15 2 10.123.123.10 208.67.222.222 internal wan1 53
4 2010-05-11 15:13:13 2 10.123.123.10 208.67.222.222 internal wan1 53
5 2010-05-11 15:13:13 2 10.123.123.10 208.67.222.222 internal wan1 53
6 2010-05-11 15:13:13 2 10.123.123.10 208.67.222.222 internal wan1 53
7 2010-05-11 15:13:11 2 10.123.123.10 208.67.222.222 internal wan1 53
8 2010-05-11 15:13:11 2 10.123.123.10 208.67.222.222 internal wan1 53
9 2010-05-11 15:13:11 2 10.123.123.10 208.67.222.222 internal wan1 53


Edit Filters
Filters
Date
Time
ID
Source
Destination
Source Interface
Destination Interface
Destination Port
Service
Sent
Received
Tran IP
[Clear All Filters]
Destination
Enable
Field Equals
NOT
Text 98.207.226.113
The destination IP address or FQDN.
OK
Cancel


FortiGate 51B
Help
Logout
System
Router
Firewall
UTM
VPN
User
WAN Opt. & Cache
Endpoint
Log&Report
Log Config
Refresh
Clear All Filters
Column Settings
Disk
Memory
Date Time ID Source Destination Source Interface Destination Interface Destination Port Service
1 2010-05-11 15:12:26 2 10.123.123.10 98.207.226.113 internal wan1 80 80/tcp 427
2 2010-05-11 15:12:24 2 10.123.123.10 98.207.226.113 internal wan1 80 80/tcp 427
3 2010-05-11 15:12:22 2 10.123.123.10 98.207.226.113 internal wan1 80 80/tcp 427
4 2010-05-11 15:11:05 2 10.123.123.10 98.207.226.113 internal wan1 80 80/tcp 427
5 2010-05-11 15:11:03 2 10.123.123.10 98.207.226.113 internal wan1 80 80/tcp 427
6 2010-05-11 15:11:01 2 10.123.123.10 98.207.226.113 internal wan1 80 80/tcp 427
7 2010-05-11 15:09:05 2 10.123.123.10 98.207.226.113 internal wan1 80 80/tcp 323



7.3 SYSLOG – Log Remoto



7.3.1 Exemplo de Log de uma Sessão de Firewall

```
May 27 20:05:38 10.123.123.1 date=2010-05-27 time=20:05:38 devname=Fortigate51B
device_id=FG50BH3G09600388 log_id=0021000002 type=traffic subtype=allowed pri
=notice status=accept vd="root" dir_disp=org tran_disp=dnat src=200.189.190.105
srcname=200.189.190.105 src_port=57788 dst=200.202.114.251 dstname=200.202.11
4.251 dst_port=80 tran_ip=10.123.123.10 tran_port=80 service=80/tcp proto=6
app_type=N/A duration=130 rule=2 policyid=2 identidx=0 sent=521 rcvd=540 shaper_d
rop_sent=0 shaper_drop_rcvd=0 perip_drop=0 shaper_sent_name="N/A"
shaper_rcvd_name="N/A" perip_name="N/A" sent_pkt=6 rcvd_pkt=4 vpn="N/A"
src_int="wan1" dst_
int="internal" SN=7358147 app="N/A" app_cat="N/A" user="N/A" group="N/A"
carrier_ep="N/A"
```

```
May 27 20:05:38 10.123.123.1 date=2010-05-27 time=20:05:38 devname=Fortigate51B
device_id=FG50BH3G09600388 log_id=0021000002 type=traffic subtype=allowed pri
=notice status=accept vd="root" dir_disp=org tran_disp=dnat src=200.189.190.105
srcname=200.189.190.105 src_port=57789 dst=200.202.114.251 dstname=200.202.11
4.251 dst_port=80 tran_ip=10.123.123.10 tran_port=80 service=80/tcp proto=6
app_type=N/A duration=130 rule=2 policyid=2 identidx=0 sent=531 rcvd=540 shaper_d
rop_sent=0 shaper_drop_rcvd=0 perip_drop=0 shaper_sent_name="N/A"
shaper_rcvd_name="N/A" perip_name="N/A" sent_pkt=6 rcvd_pkt=4 vpn="N/A"
src_int="wan1" dst_
int="internal" SN=7358148 app="N/A" app_cat="N/A" user="N/A" group="N/A"
carrier_ep="N/A"
```

7.3.2 Exemplo de Log de uma Sessão de IPS

```
May 27 20:05:38 10.123.123.1 date=2010-05-27 time=20:05:38 devname=Fortigate51B
device_id=FG50BH3G09600388 log_id=0419016384 type=ips subtype=signature pri=a
lert severity=medium carrier_ep="N/A" vd="" vd="" profile="N/A" src=200.189.190.105
dst=10.123.123.10 src_int="wan1" dst_int="internal" policyid=2 identidx=0
 serial=7368475 status=detected proto=6 service=http vd="root" count=1
src_port=40881 dst_port=80 attack_id=12709 sensor="My_IPS_Sensor"
ref="http://www.fort
inet.com/ids/VID12709" user="N/A" group="N/A" incident_serialno=286557658
msg="web_server: IISadmpwd.aexp.Usage"

May 27 20:05:38 10.123.123.1 date=2010-05-27 time=20:05:38 devname=Fortigate51B
device_id=FG50BH3G09600388 log_id=0419016384 type=ips subtype=signature pri=a
lert severity=medium carrier_ep="N/A" vd="" vd="" profile="N/A" src=200.189.190.105
dst=10.123.123.10 src_int="wan1" dst_int="internal" policyid=2 identidx=0
 serial=7368478 status=detected proto=6 service=http vd="root" count=1
src_port=40884 dst_port=80 attack_id=12709 sensor="My_IPS_Sensor"
ref="http://www.fort
inet.com/ids/VID12709" user="N/A" group="N/A" incident_serialno=286557661
msg="web_server: IISadmpwd.aexp.Usage"
```

7.3.3 Exemplo de Configuração de Servidor syslog-ng

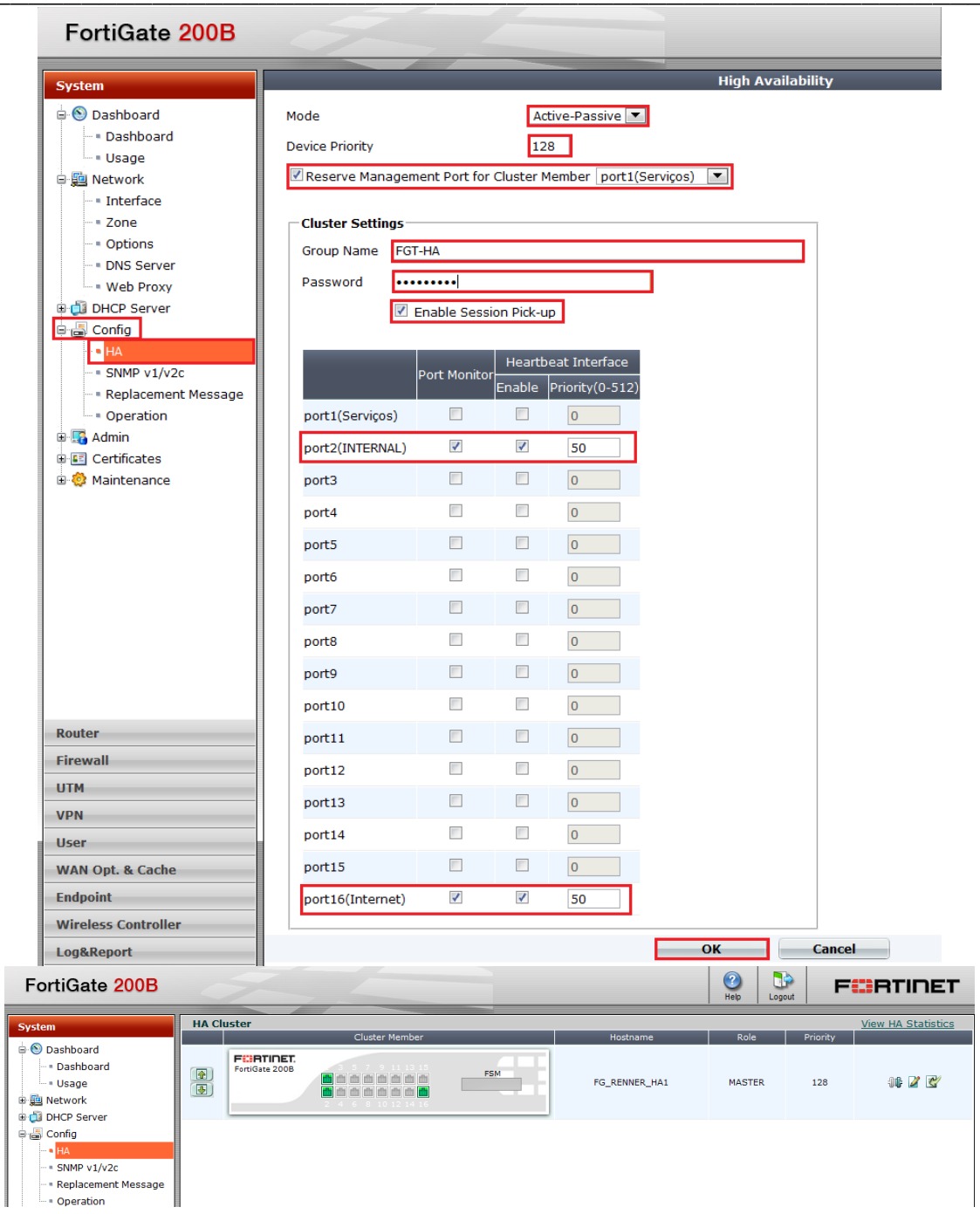
Adicionar ao arquivo /etc/syslog-ng/syslog-ng.conf as linhas abaixo:

```
source remote_fortigate { udp(); };
filter filter_fortigate { netmask(10.123.123.1/32); };
destination df_fortigate { file("/var/log/fortigate.log"); };
log {
     source(remote_fortigate);
     filter(filter_fortigate);
     destination(df_fortigate);
```

```
};
```

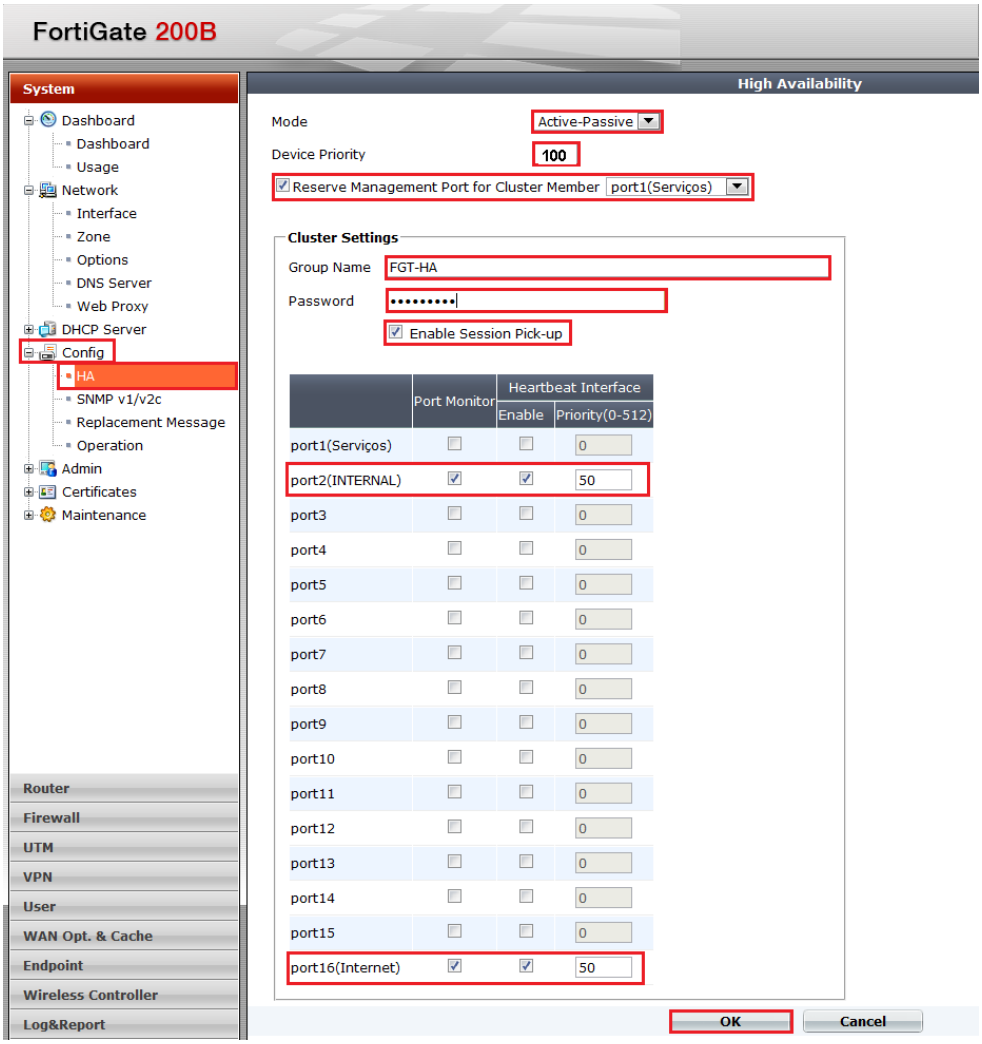
8 Alta Disponibilidade – High Availability (HA)

Configuração do Master:

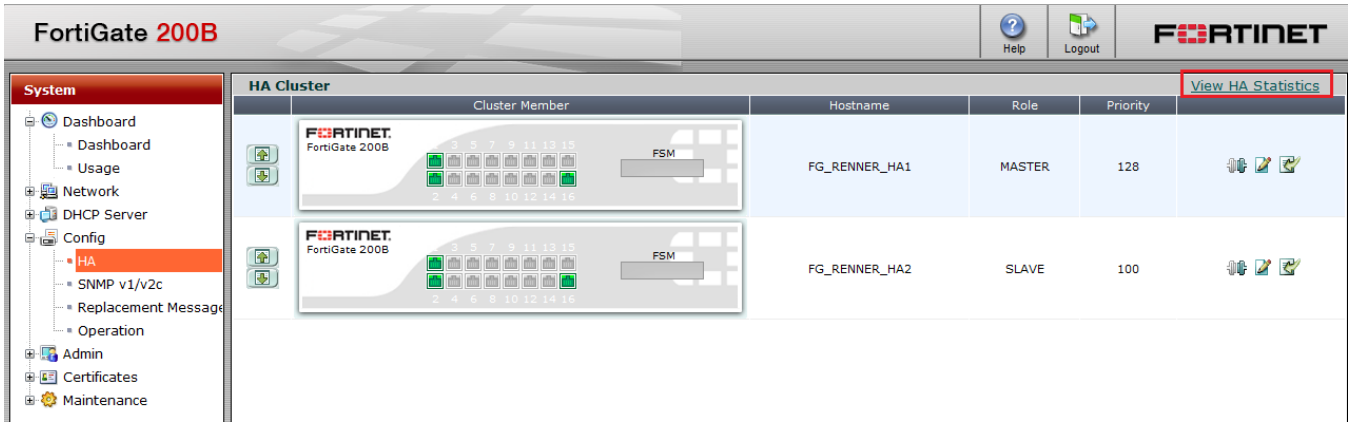

FortiGate 200B
System
Dashboard
Dashboard
Usage
Network
Interface
Zone
Options
DNS Server
Web Proxy
DHCP Server
Config
HA
SNMP v1/v2c
Replacement Message
Operation
Admin
Certificates
Maintenance
Router
Firewall
UTM
VPN
User
WAN Opt. & Cache
Endpoint
Wireless Controller
Log&Report
High Availability
Mode
Active-Passive
Device Priority
128
Reserve Management Port for Cluster Member
port1(Serviços)
Cluster Settings
Group Name
FGT-HA
Password
Enable Session Pick-up
Port Monitor
Heartbeat Interface
Enable
Priority(0-512)
port1(Serviços)
port2(INTERNAL)
50
port3
port4
port5
port6
port7
port8
port9
port10
port11
port12
port13
port14
port15
port16(Internet)
50
OK
Cancel
FortiGate 200B
Help
Logout
FORTINET
System
Dashboard
Dashboard
Usage
Network
DHCP Server
Config
HA
SNMP v1/v2c
Replacement Message
Operation
HA Cluster
View HA Statistics
Cluster Member
Hostname
Role
Priority
FortiGate 200B
FSM
FG_RENNER_HA1
MASTER
128

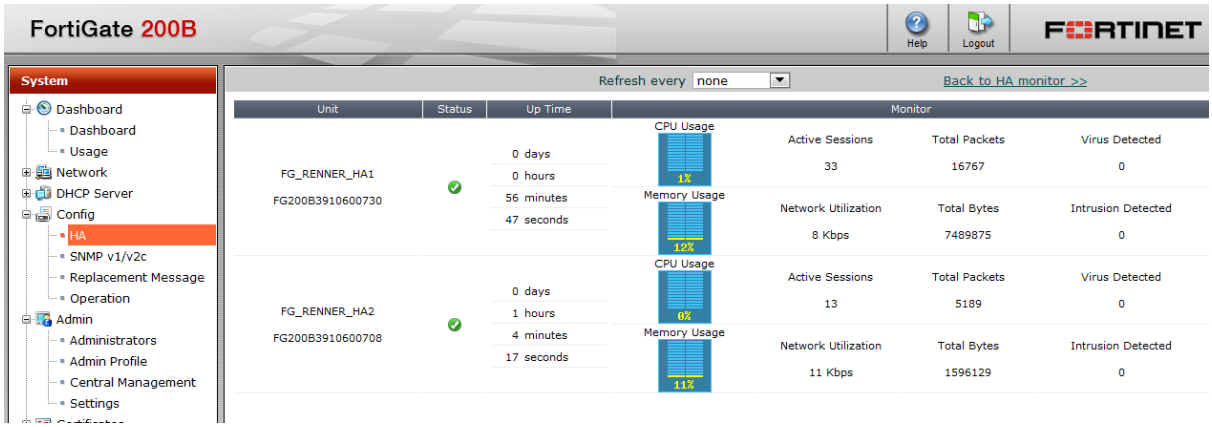
No Slave:

- Observar password e priority (o slave deve possuir um valor menor que o do master).



Verificar status do cluster HA no Master:





Pode-se conectar ao firewall slave através da command line. O comando abaixo pode ser utilizado para descobrir o id do slave:

```
FG_RENNER_HA1 # execute ha manage ?
<id>    please input peer box index.
<1>     Subsidary unit FG200B3910600708
```

Para se conectar ao slave de ID 1 usar o comando abaixo:

```
FG_RENNER_HA1 # execute ha manage 1

FG_RENNER_HA2 $
```

8.1 MAC Address em cluster HA

Quando um equipamento é configurado para operar em um cluster HA o MAC address das suas interfaces é modificado.

O comando "diagnose hardware deviceinfo nic <port>" pode ser usado para verificar qual era o antigo MAC (permanent) e o atual (current):

```
# diagnose hardware deviceinfo nic port1
Description             mvl_sw Ethernet driver1.0
System_Device_Name      port1
CPU_port                10
vlanid                  1
FID                     1
num_ports               1
member                  0x0001
cfg                     0-0x0
Current_HWaddr          00:09:0f:09:00:00
Permanent_HWaddr        00:09:0f:d6:da:a3
State                   up
Link                    up
Speed                   100
Duplex                  full
Rx_Packets              5618605
Tx_Packets              73267810
Rx_Bytes                504060403
Tx_Bytes                22798186279
```

8.2 Verificação de Status Através da CLI

O comando "get system ha" pode ser usado para verificar o status do cluster HA:

```
# get system ha
group-id            : 0
group-name          : FG-HA-VHOST
mode                : a-p
password            : *
hbdev               : "port10" 50 "port15" 50 "port16" 50
session-sync-dev    :
route-ttl           : 10
route-wait          : 0
route-hold          : 10
sync-config         : enable
encryption          : disable
authentication      : disable
hb-interval         : 2
hb-lost-threshold   : 6
helo-holddown       : 20
```

```
arps                  : 5
arps-interval         : 8
session-pickup        : enable
session-pickup-delay: disable
link-failed-signal    : disable
uninterruptable-upgrade: enable
ha-mgmt-status        : disable
ha-eth-type           : 8890
hc-eth-type           : 8891
l2ep-eth-type         : 8893
ha-uptime-diff-margin: 300
vcluster2             : disable
vcluster-id           : 1
override              : disable
priority              : 128
monitor               : "port10" "port15" "port16"
pingserver-monitor-interface:
pingserver-failover-threshold: 0
pingserver-flip-timeout: 60
vdom                  : "VDOM1" "VDOM9" "root"
```

9 VPN IPSEC – Client-to-Site

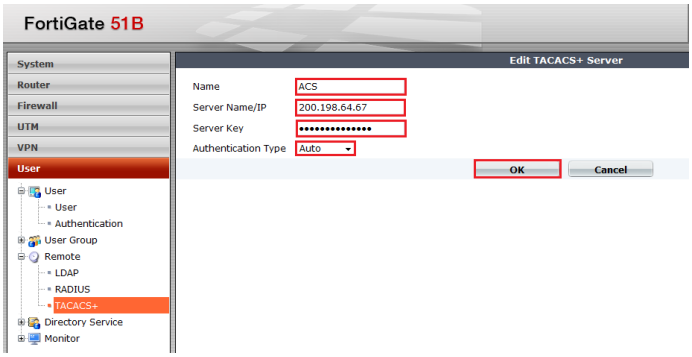
O Fortigate pode autenticar usuário de VPN IPSec de duas formas:

- Método 1: pre-shared key + usuário + password - neste caso o usuário e conta são obtidos em um servidor TACACS+ ou RADIUS. ***OBS:** **Não é possível fazer a autenticação desta forma com uma conta local (usuário + password) sendo obrigatório o uso de um servidor Tacacs+/Radius (Ex: Cisco ACS).***

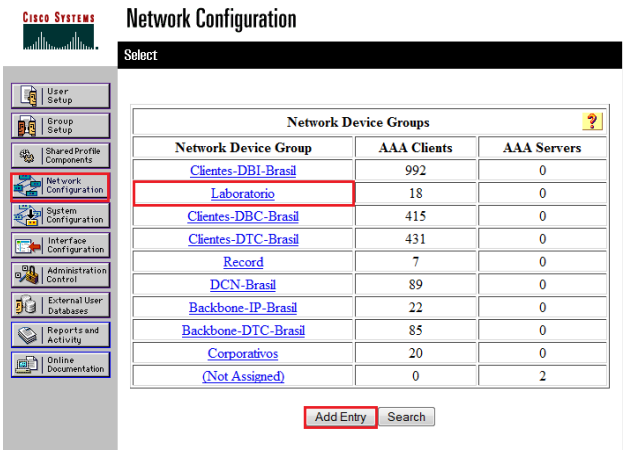
- Método 2: apenas pre-shared key - neste caso o usuários não será requisitado a informar o usuário e senha, bastando apenas apresentar a pre-shared key.

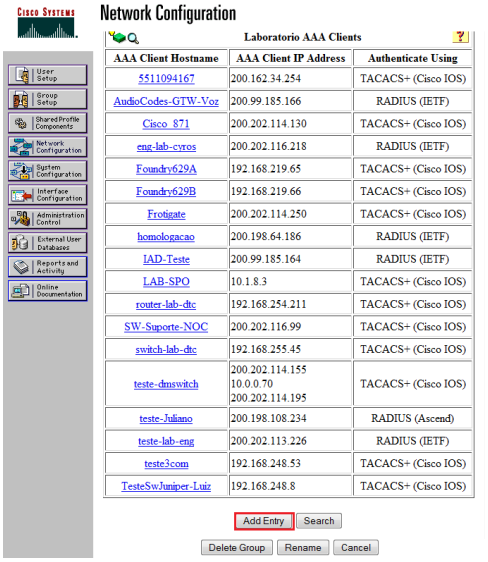
9.1 VPN IPSEC – Client-to-Site – Método 1

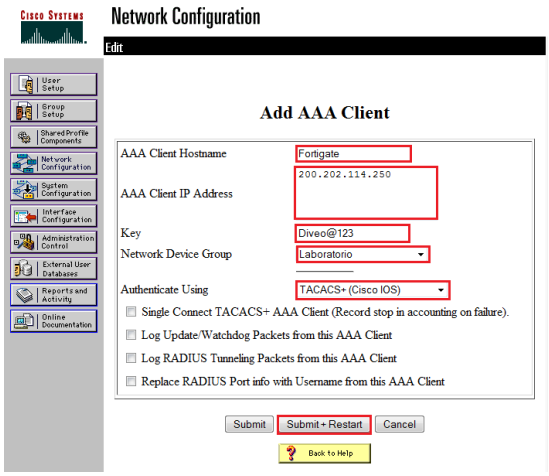
9.1.1 Servidor TACACS+



As telas abaixo apresentam as configurações realizadas no Cisco ACS:

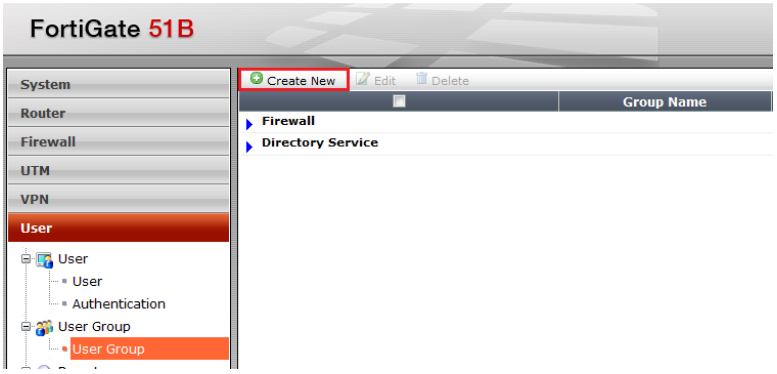


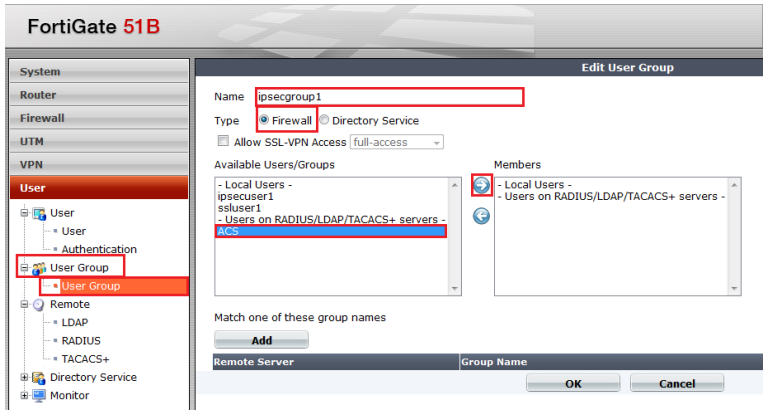


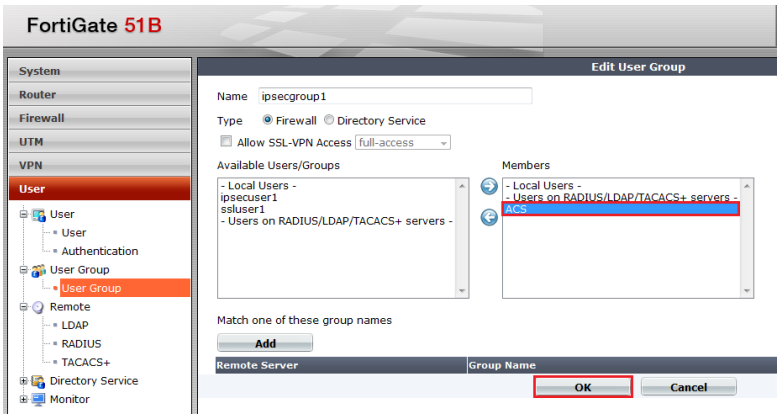


*Obs: O campo “Key” deve ser preenchido com o mesmo valor usado no campo “Server Key” da configuração do Fortigate.

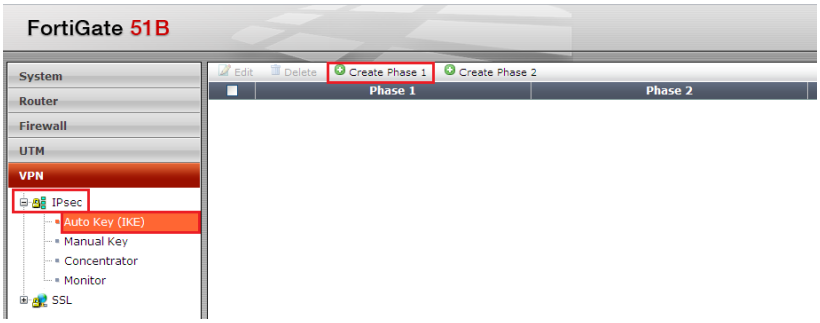
9.1.2 Grupo de Usuários da VPN IPSEC

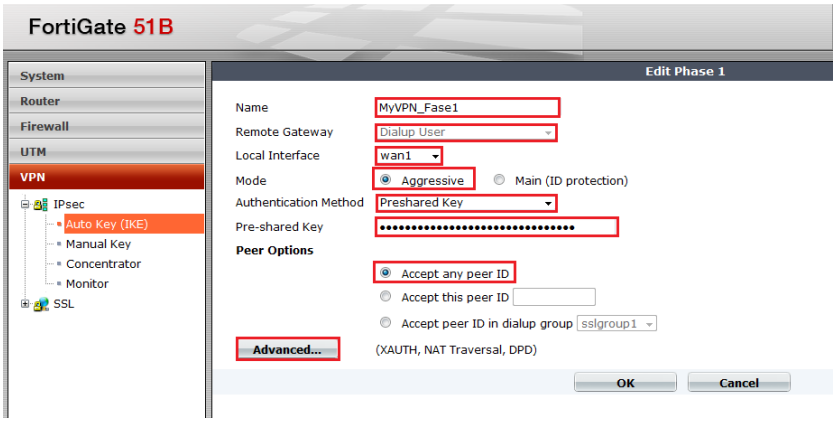


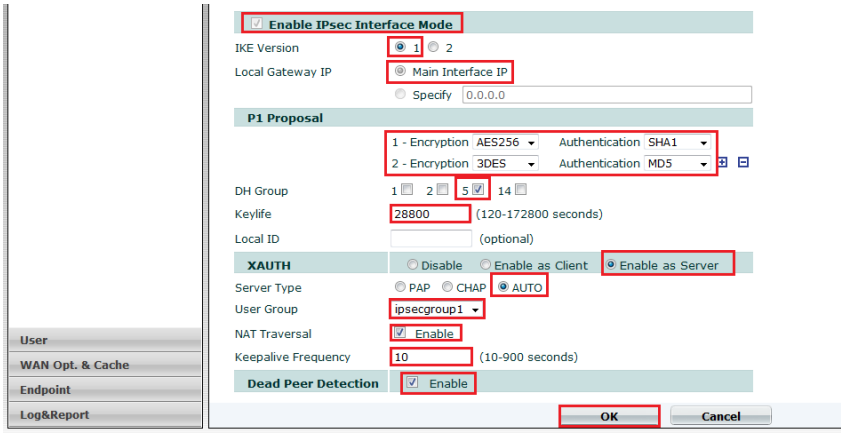




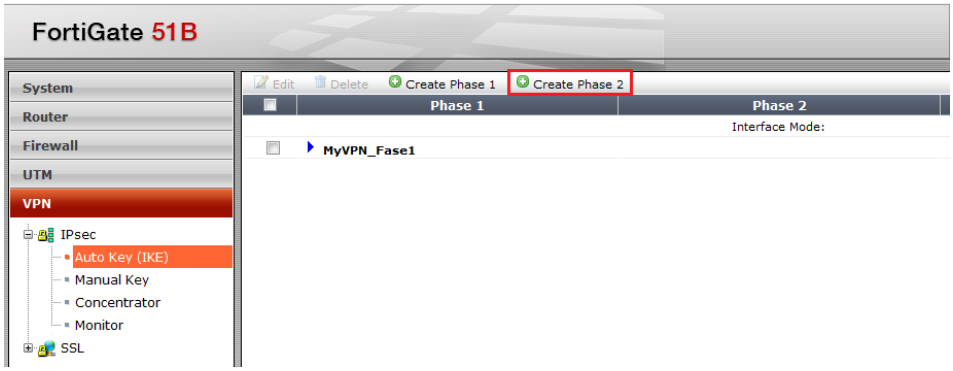
9.1.3 Fase 1

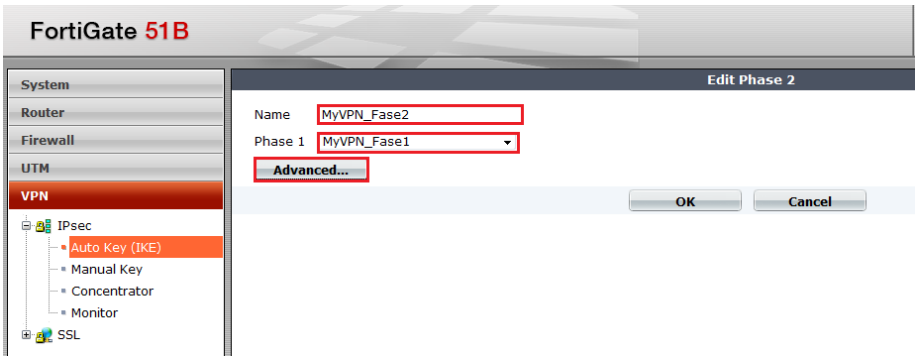

FortiGate 51B
System
Router
Firewall
UTM
VPN
IPsec
Auto Key (IKE)
Manual Key
Concentrator
Monitor
SSL
Edit
Delete
Create Phase 1
Create Phase 2
Phase 1
Phase 2

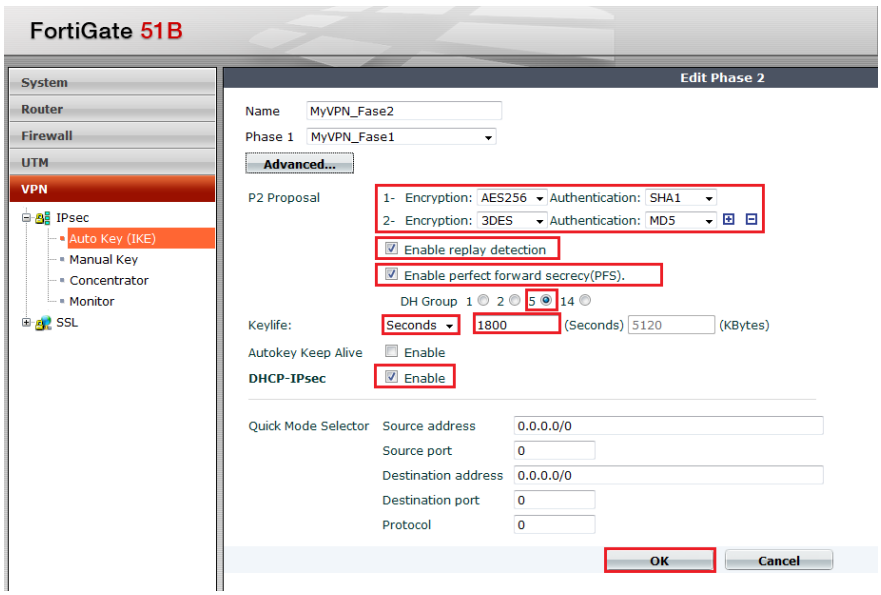

FortiGate 51B
System
Router
Firewall
UTM
VPN
IPsec
Auto Key (IKE)
Manual Key
Concentrator
Monitor
SSL
Edit Phase 1
Name
MyVPN_Fase1
Remote Gateway
Dialup User
Local Interface
wan1
Mode
Aggressive
Main (ID protection)
Authentication Method
Preshared Key
Pre-shared Key
Peer Options
Accept any peer ID
Accept this peer ID
Accept peer ID in dialup group
sslgroup1
Advanced...
(XAUTH, NAT Traversal, DPD)
OK
Cancel


Enable IPsec Interface Mode
IKE Version
1
2
Local Gateway IP
Main Interface IP
Specify
0.0.0.0
P1 Proposal
1 - Encryption
AES256
Authentication
SHA1
2 - Encryption
3DES
Authentication
MD5
DH Group
1
2
5
14
Keylife
28800
(120-172800 seconds)
Local ID
(optional)
XAUTH
Disable
Enable as Client
Enable as Server
Server Type
PAP
CHAP
AUTO
User Group
ipsecgroup1
NAT Traversal
Enable
Keepalive Frequency
10
(10-900 seconds)
Dead Peer Detection
Enable
OK
Cancel
User
WAN Opt. & Cache
Endpoint
Log&Report

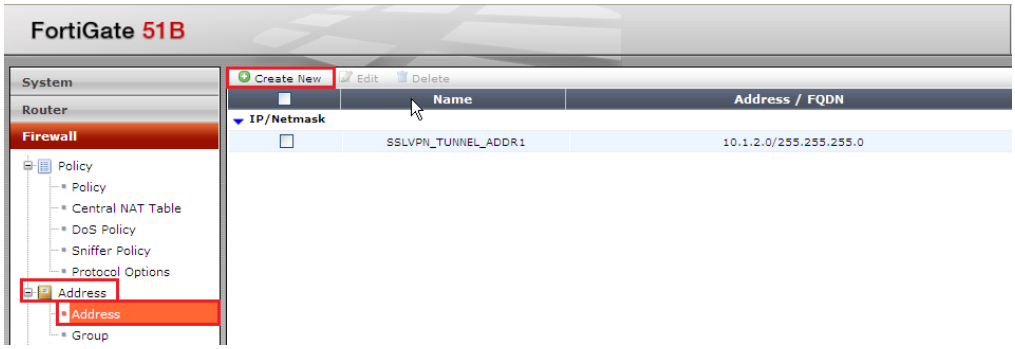
9.1.4 Fase 2

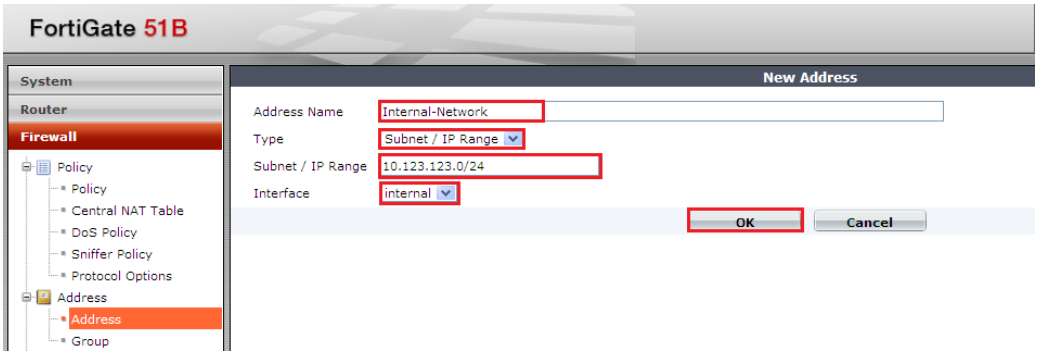

FortiGate 51B
System
Router
Firewall
UTM
VPN
IPsec
Auto Key (IKE)
Manual Key
Concentrator
Monitor
SSL
Edit
Delete
Create Phase 1
Create Phase 2
Phase 1
Phase 2
Interface Mode:
MyVPN_Fase1

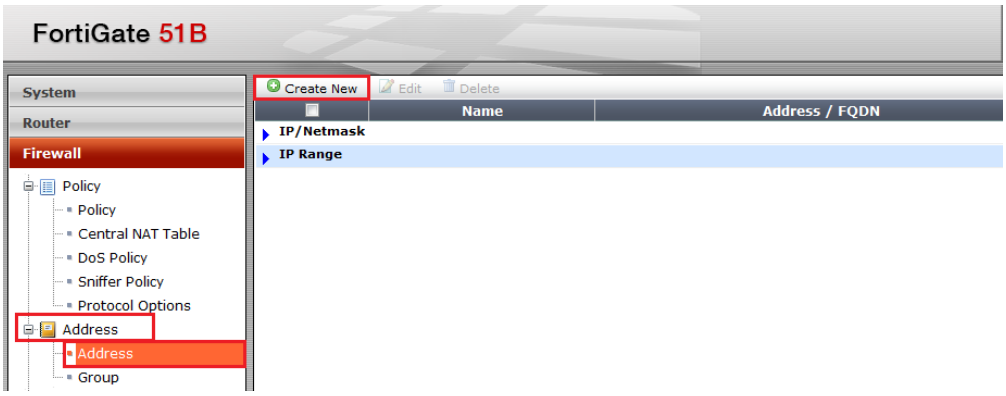

FortiGate 51B
System
Router
Firewall
UTM
VPN
IPsec
Auto Key (IKE)
Manual Key
Concentrator
Monitor
SSL
Edit Phase 2
Name
MyVPN_Fase2
Phase 1
MyVPN_Fase1
Advanced...
OK
Cancel

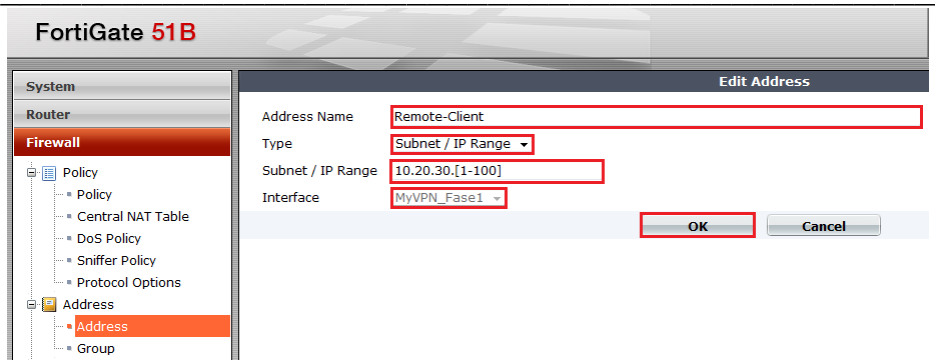

FortiGate 51B
System
Router
Firewall
UTM
VPN
IPsec
Auto Key (IKE)
Manual Key
Concentrator
Monitor
SSL
Edit Phase 2
Name
MyVPN_Fase2
Phase 1
MyVPN_Fase1
Advanced...
P2 Proposal
1- Encryption: AES256 Authentication: SHA1
2- Encryption: 3DES Authentication: MD5
Enable replay detection
Enable perfect forward secrecy(PFS).
DH Group 1 2 5 14
Keylife:
Seconds
1800
(Seconds)
5120
(KBytes)
Autokey Keep Alive
Enable
DHCP-IPsec
Enable
Quick Mode Selector
Source address
0.0.0.0/0
Source port
0
Destination address
0.0.0.0/0
Destination port
0
Protocol
0
OK
Cancel

9.1.5 Endereços da Rede Interna e Range dos Remote Clients



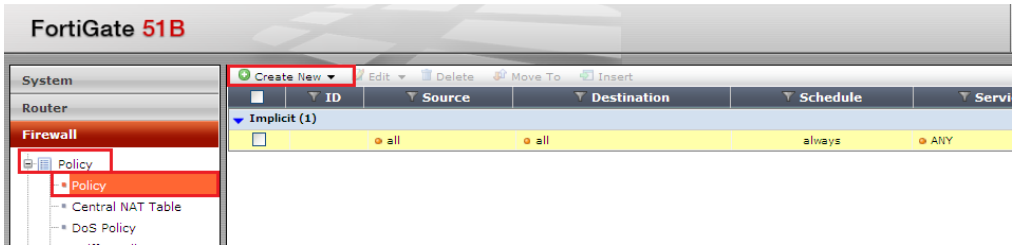




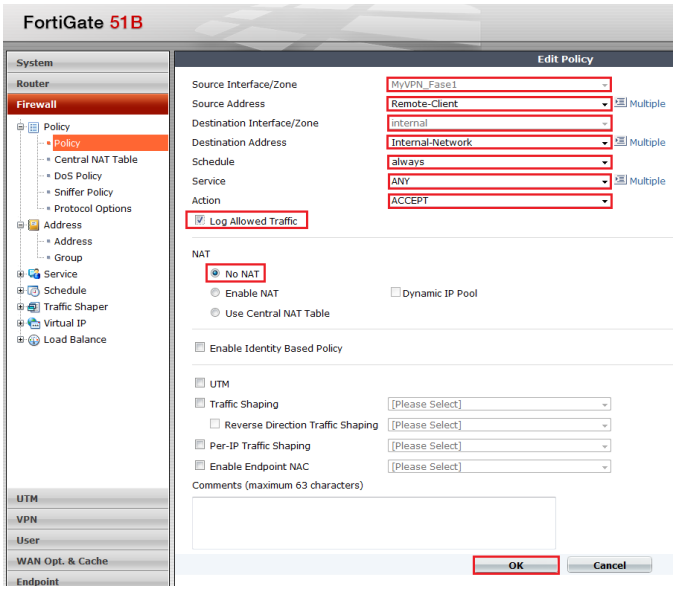


9.1.6 Regra de VPN

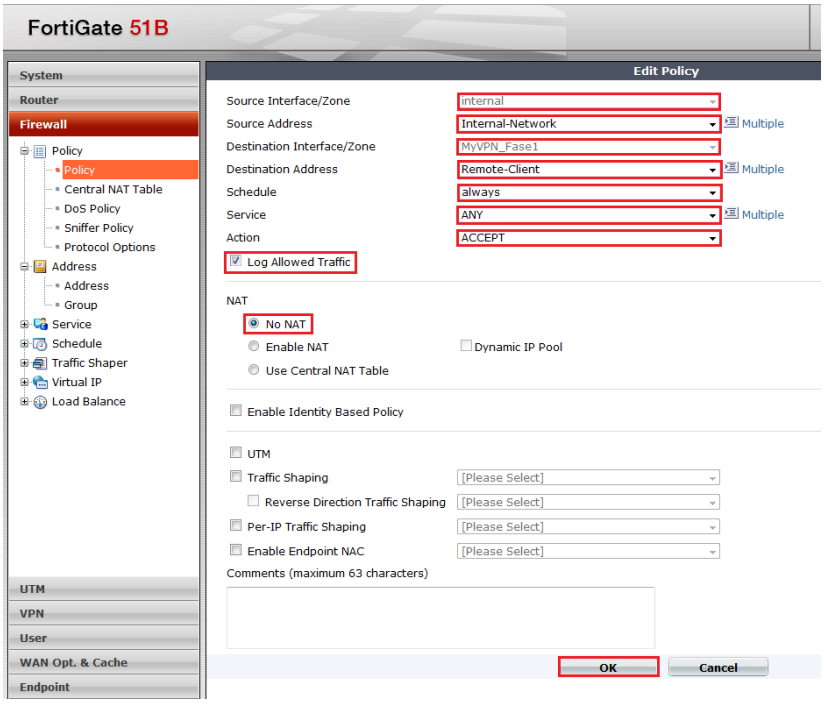
***Observação: A regra de VPN deve ficar acima de qualquer outra regra que possua endereços de origem e destino similares.**

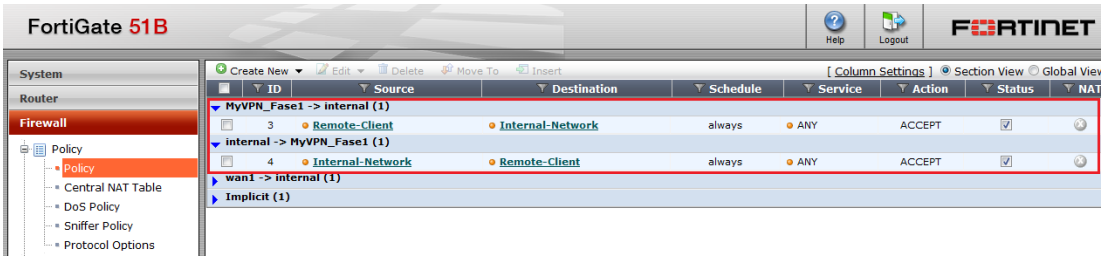


Regra de entrada:



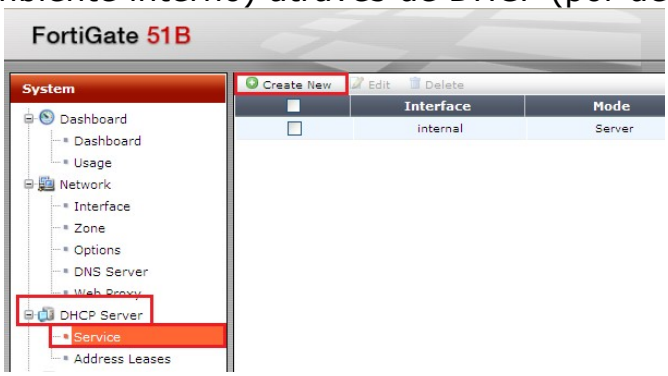
Regra de saída (retorno):

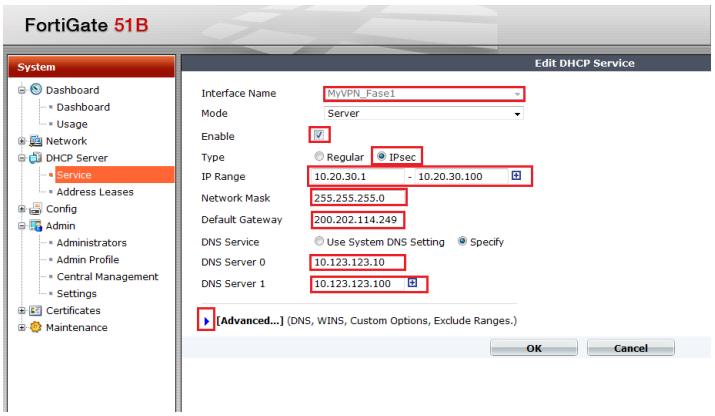


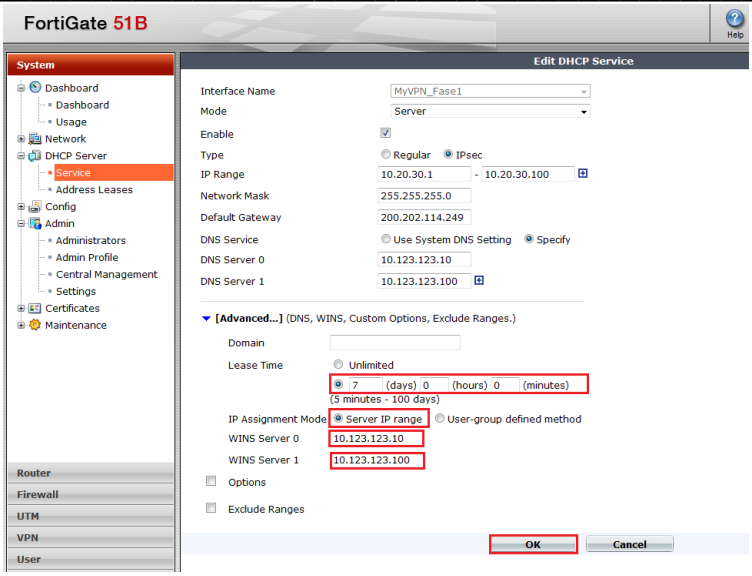


9.1.7 DHCP para Remote Clients

Os usuários remotos, ao se conectarem à VPN, receberão seus endereços locais (usados dentro do ambiente interno) através de DHCP (por dentro do túnel IPSec).

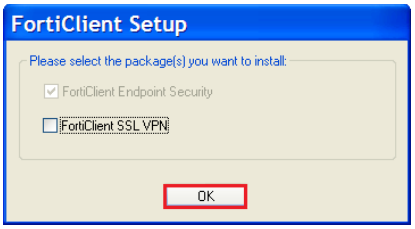


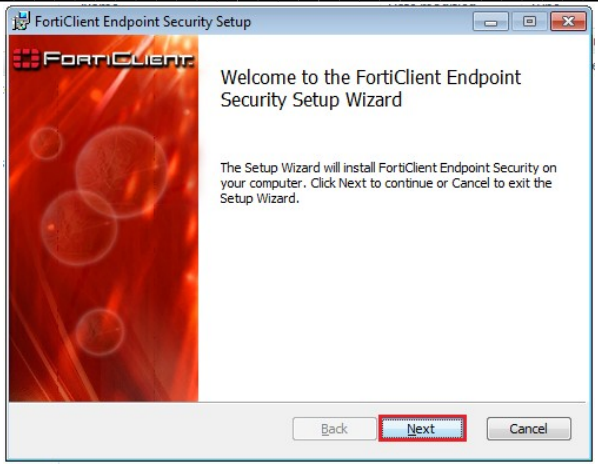


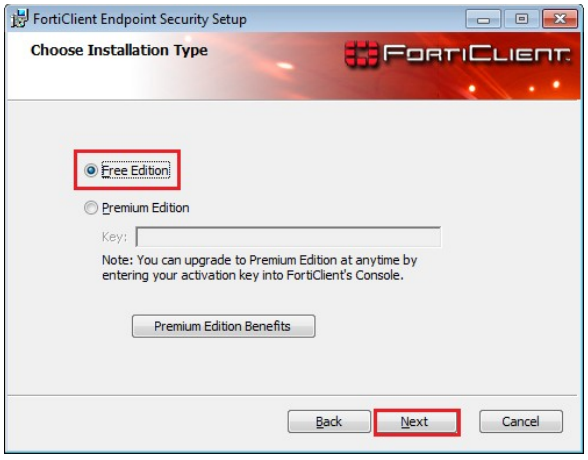


9.1.8 Instalação do FortiClient Endpoint Security Application

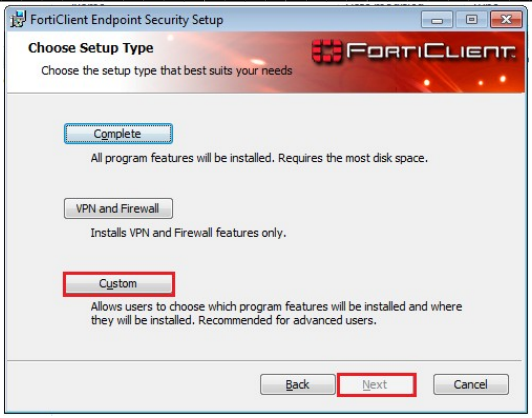
Fazer o download da versão "free" em: http://www.forticlient.com/



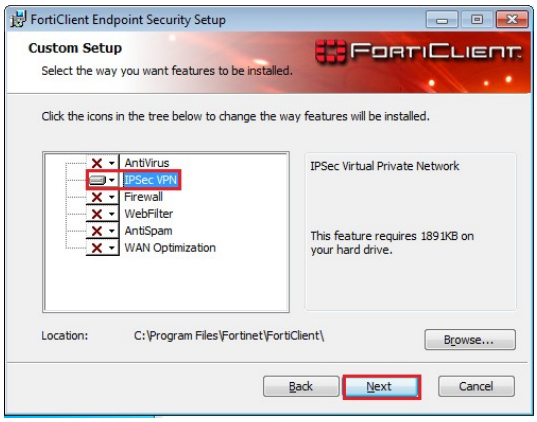

FortiClient Endpoint Security Setup
FortiClient
Welcome to the FortiClient Endpoint Security Setup Wizard
The Setup Wizard will install FortiClient Endpoint Security on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Back
Next
Cancel

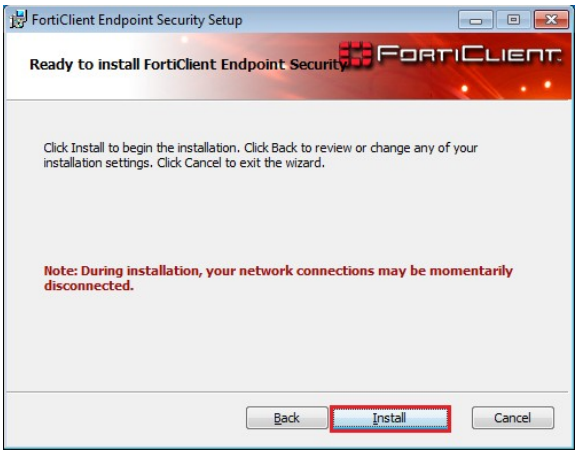

FortiClient Endpoint Security Setup
Choose Installation Type
FortiClient
Free Edition
Premium Edition
Key:
Note: You can upgrade to Premium Edition at anytime by entering your activation key into FortiClient's Console.
Premium Edition Benefits
Back
Next
Cancel

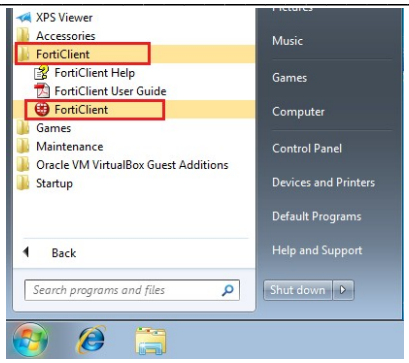

FortiClient Endpoint Security Setup
End-User License Agreement
Please read the following license agreement carefully
FortiClient
End User License Agreement for FortiClient
NOTICE TO ALL USERS: PLEASE READ THE TERMS AND CONDITIONS OF THE LICENSE AGREEMENT CAREFULLY. FORTINET, INC. IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER
I accept the terms in the License Agreement
Print
Back
Next
Cancel

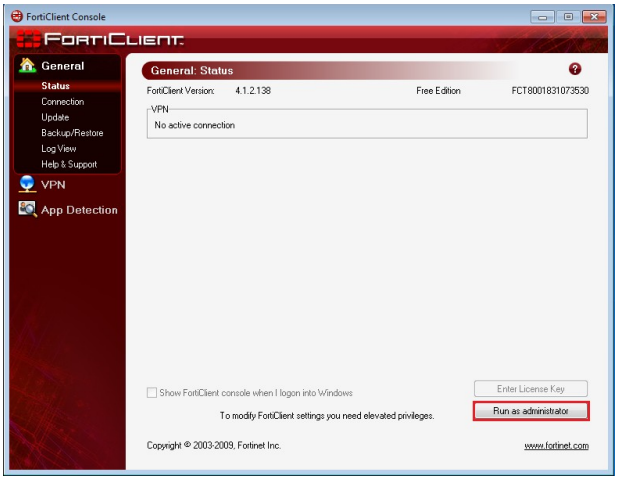


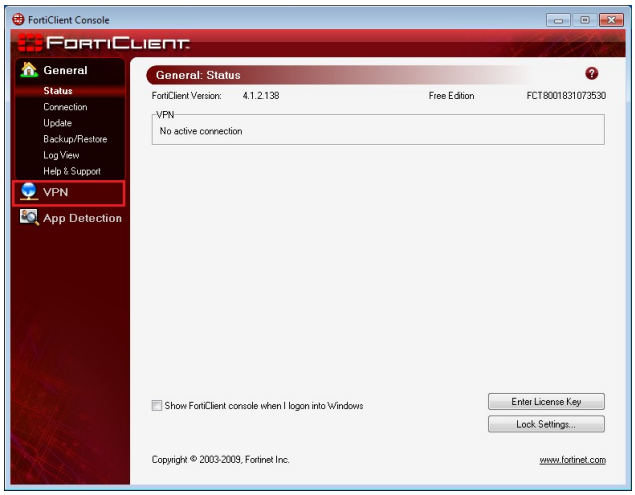
Desabilitar todos os serviços, exceto o VPN IPSec:

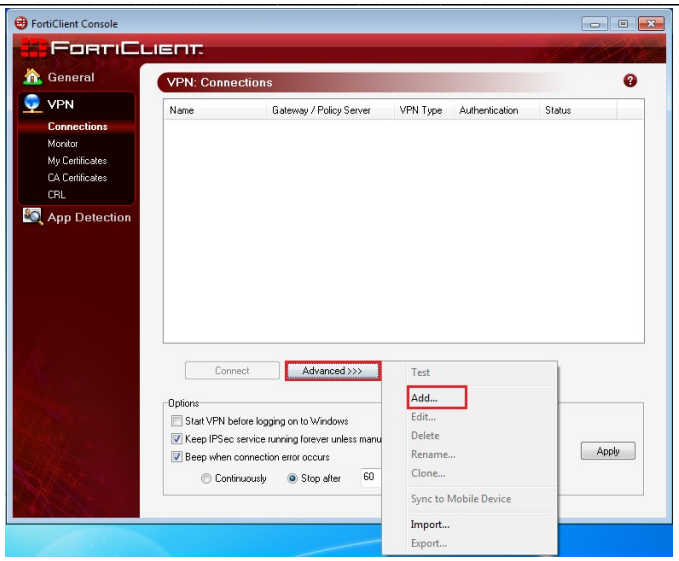


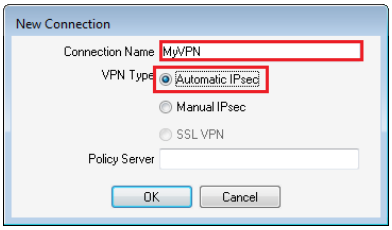


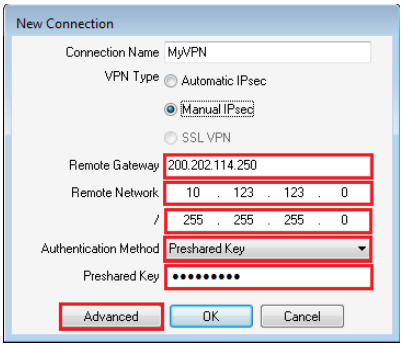

XPS Viewer
Accessories
FortiClient
FortiClient Help
FortiClient User Guide
FortiClient
Games
Maintenance
Oracle VM VirtualBox Guest Additions
Startup
Back
Search programs and files
Music
Games
Computer
Control Panel
Devices and Printers
Default Programs
Help and Support
Shut down

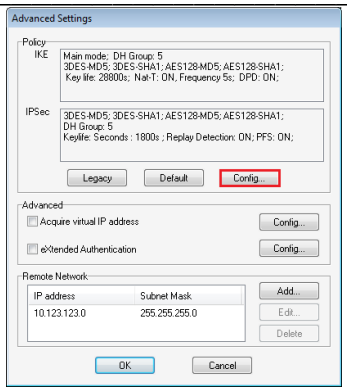

FortiClient Console
FortiClient
General
Status
Connection
Update
Backup/Restore
Log View
Help & Support
VPN
App Detection
General: Status
FortiClient Version: 4.1.2.138
Free Edition
FCT8001831073530
VPN
No active connection
Show FortiClient console when I logon into Windows
Enter License Key
To modify FortiClient settings you need elevated privileges.
Run as administrator
Copyright © 2003-2009, Fortinet Inc.
www.fortinet.com


FortiClient Console
FortiClient
General
Status
Connection
Update
Backup/Restore
Log View
Help & Support
VPN
App Detection
General: Status
FortiClient Version: 4.1.2.138
Free Edition
FCT8001831073530
VPN
No active connection
Show FortiClient console when I logon into Windows
Enter License Key
Lock Settings...
Copyright © 2003-2009, Fortinet Inc.
www.fortinet.com

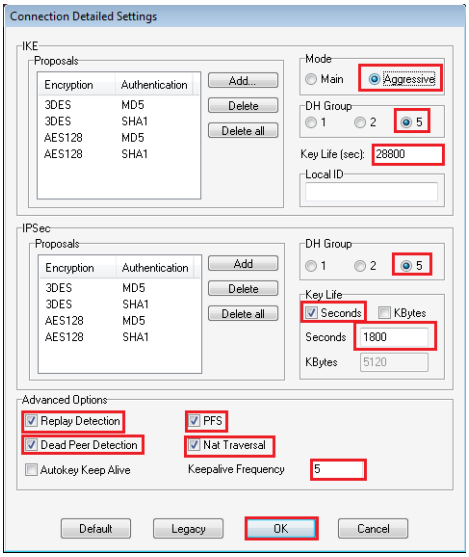

FortiClient Console
FortiClient
General
VPN
Connections
Monitor
My Certificates
CA Certificates
CRL
App Detection
VPN: Connections
Name
Gateway / Policy Server
VPN Type
Authentication
Status
Connect
Advanced >>>
Test
Add...
Edit...
Delete
Rename...
Clone...
Sync to Mobile Device
Import...
Export...
Options
Start VPN before logging on to Windows
Keep IPSec service running forever unless manu
Beep when connection error occurs
Continuously
Stop after
60
Apply

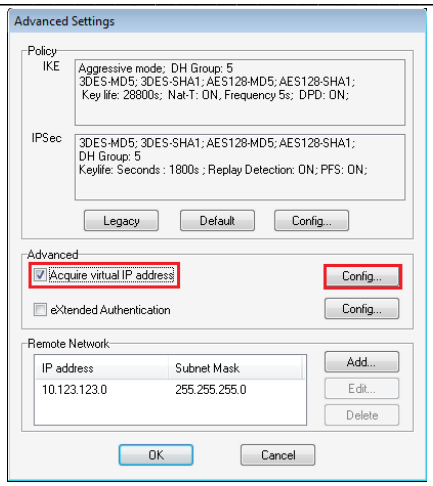

New Connection
Connection Name
MyVPN
VPN Type
Automatic IPsec
Manual IPsec
SSL VPN
Policy Server
OK
Cancel

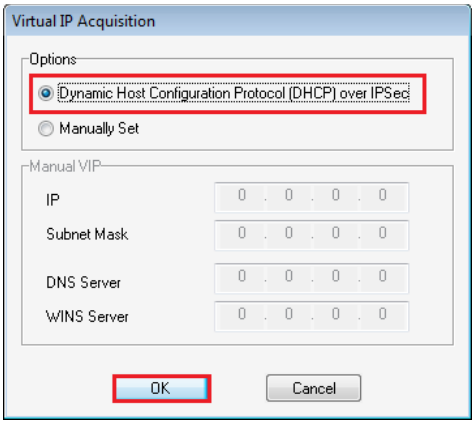

New Connection
Connection Name
MyVPN
VPN Type
Automatic IPsec
Manual IPsec
SSL VPN
Remote Gateway
200.202.114.250
Remote Network
10 . 123 . 123 . 0
/
255 . 255 . 255 . 0
Authentication Method
Preshared Key
Preshared Key
Advanced
OK
Cancel

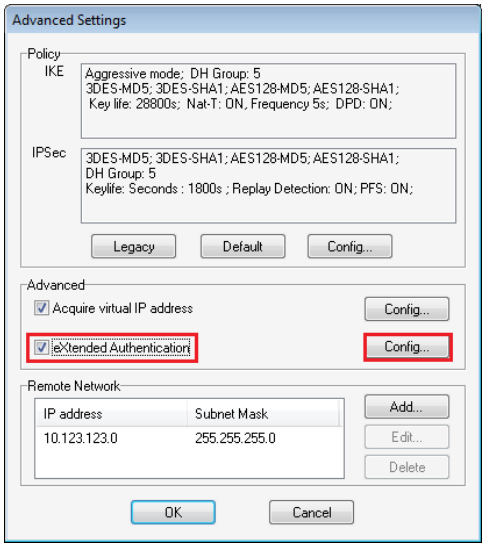


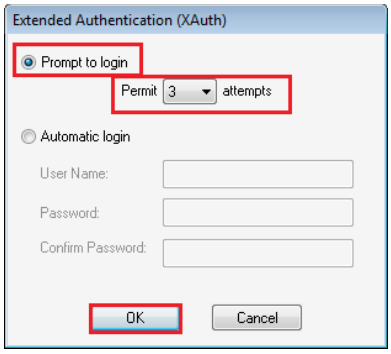
*Obs: O mode deve ser ajustado para Aggressive (como definido na Fase1 – 8.1.3).



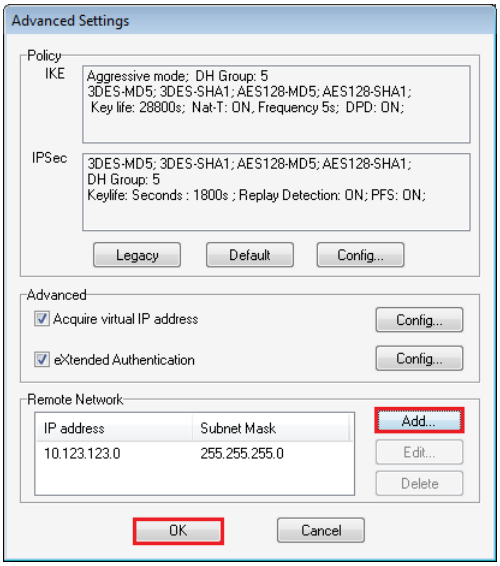

Advanced Settings
Policy
IKE
Aggressive mode; DH Group: 5
3DES-MD5; 3DES-SHA1; AES128-MD5; AES128-SHA1;
Key life: 28800s; Nat-T: ON, Frequency 5s; DPD: ON;
IPSec
3DES-MD5; 3DES-SHA1; AES128-MD5; AES128-SHA1;
DH Group: 5
Keylife: Seconds : 1800s ; Replay Detection: ON; PFS: ON;
Legacy
Default
Config...
Advanced
Acquire virtual IP address
Config...
eXtended Authentication
Config...
Remote Network
IP address
Subnet Mask
10.123.123.0
255.255.255.0
Add...
Edit...
Delete
OK
Cancel

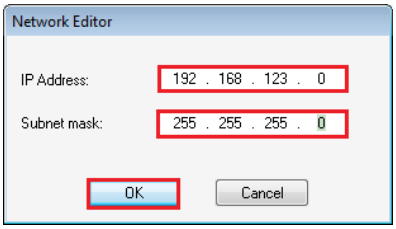

Virtual IP Acquisition
Options
Dynamic Host Configuration Protocol (DHCP) over IPSec
Manually Set
Manual VIP
IP
Subnet Mask
DNS Server
WINS Server
0 . 0 . 0 . 0
OK
Cancel

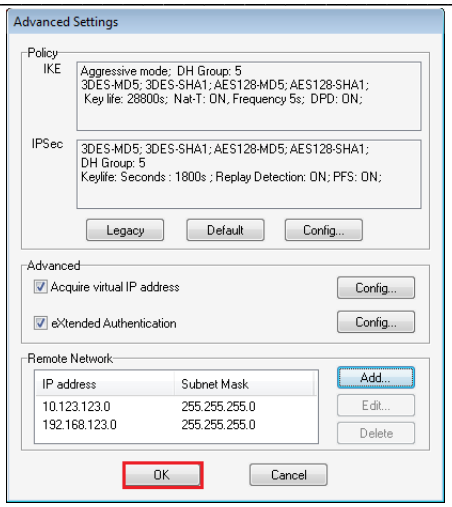

Advanced Settings
Policy
IKE
Aggressive mode; DH Group: 5
3DES-MD5; 3DES-SHA1; AES128-MD5; AES128-SHA1;
Key life: 28800s; Nat-T: ON, Frequency 5s; DPD: ON;
IPSec
3DES-MD5; 3DES-SHA1; AES128-MD5; AES128-SHA1;
DH Group: 5
Keylife: Seconds : 1800s ; Replay Detection: ON; PFS: ON;
Legacy
Default
Config...
Advanced
Acquire virtual IP address
Config...
eXtended Authentication
Config...
Remote Network
IP address
Subnet Mask
10.123.123.0
255.255.255.0
Add...
Edit...
Delete
OK
Cancel

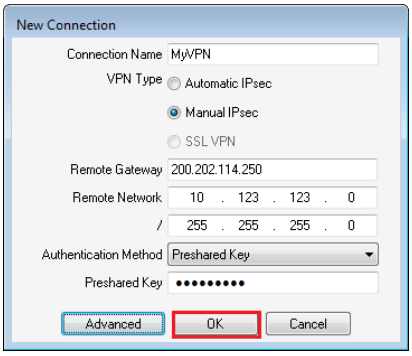


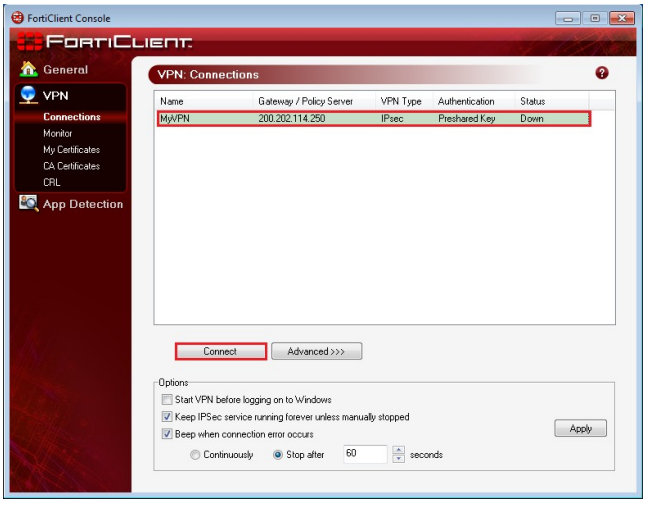
Caso existam mais redes a serem acessadas através da VPN.



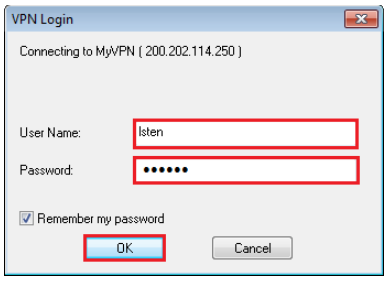



Advanced Settings
Policy
IKE
Aggressive mode; DH Group: 5
3DES-MD5; 3DES-SHA1; AES128-MD5; AES128-SHA1;
Key life: 28800s; Nat-T: ON, Frequency 5s; DPD: ON;
IPSec
3DES-MD5; 3DES-SHA1; AES128-MD5; AES128-SHA1;
DH Group: 5
Keylife: Seconds : 1800s ; Replay Detection: ON; PFS: ON;
Legacy
Default
Config...
Advanced
Acquire virtual IP address
Config...
eXtended Authentication
Config...
Remote Network
IP address
Subnet Mask
10.123.123.0
255.255.255.0
192.168.123.0
255.255.255.0
Add...
Edit...
Delete
OK
Cancel

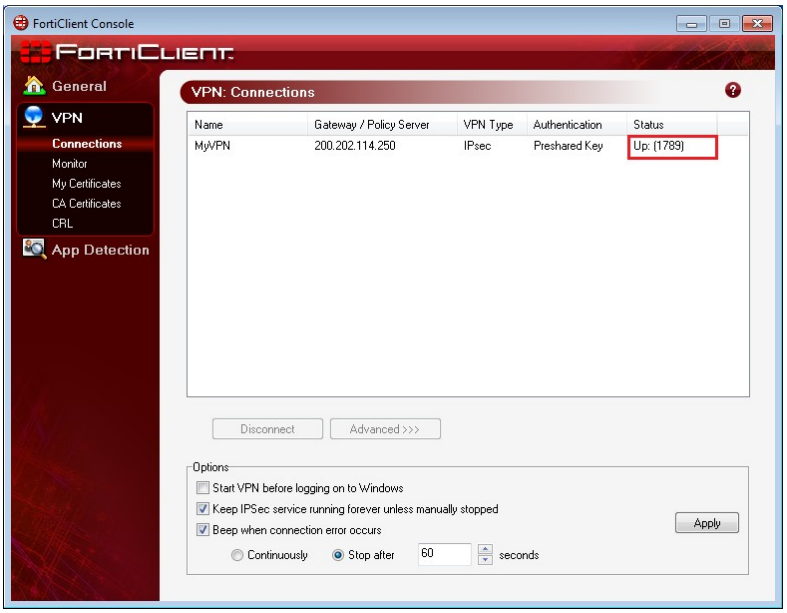

New Connection
Connection Name MyVPN
VPN Type
Automatic IPsec
Manual IPsec
SSL VPN
Remote Gateway 200.202.114.250
Remote Network 10 . 123 . 123 . 0
/ 255 . 255 . 255 . 0
Authentication Method Preshared Key
Preshared Key
Advanced
OK
Cancel


FortiClient Console
FortiClient
General
VPN
Connections
Monitor
My Certificates
CA Certificates
CRL
App Detection
VPN: Connections
Name
Gateway / Policy Server
VPN Type
Authentication
Status
MyVPN
200.202.114.250
IPsec
Preshared Key
Down
Connect
Advanced >>>
Options
Start VPN before logging on to Windows
Keep IPSec service running forever unless manually stopped
Beep when connection error occurs
Apply
Continuously
Stop after
60
seconds

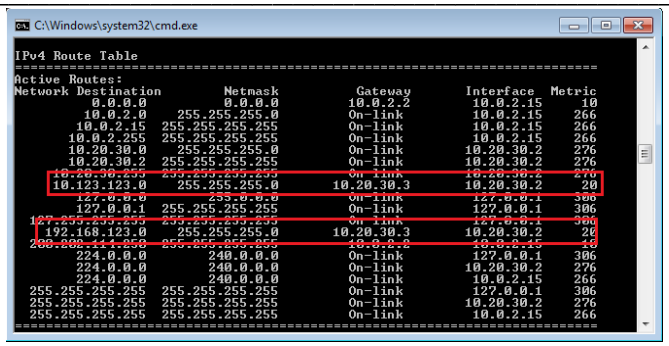
Usar algum usuário existente no servidor TACACS+ (ACS) para fazer o login:



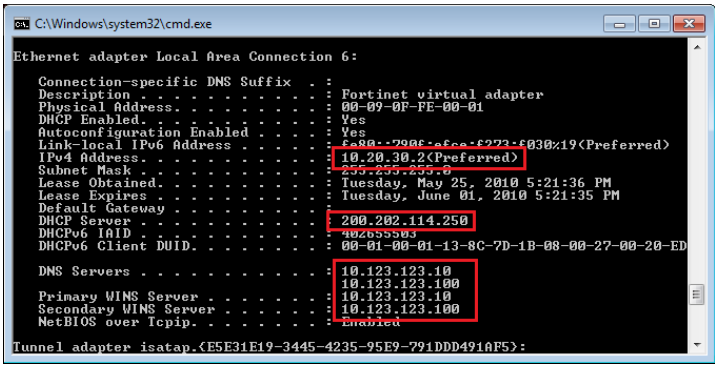
Conexão estabelecida com sucesso:



Saída do comando *netstat –rnv* :



Saída do comando *ipconfig /all* :



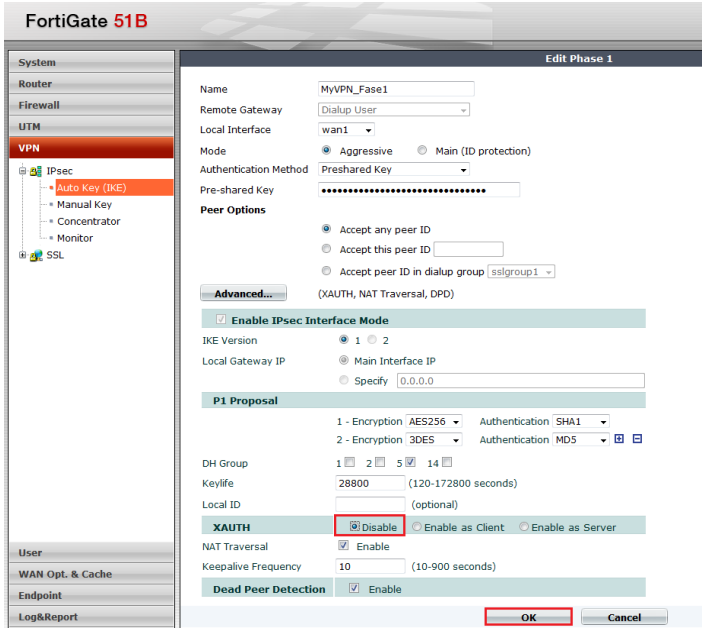
9.2 VPN IPSEC – Client-to-Site – Método 2

Neste segundo metódo a autenticação do usuário é realizada apenas através de um chave previamente compartilhada (pré-shared key).

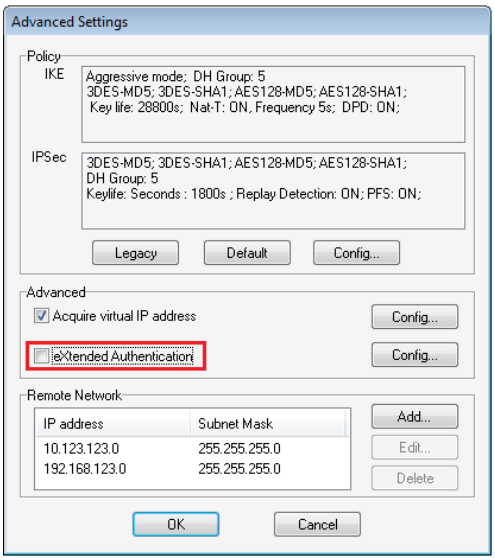
Este método tem como vantagem a facilidade de configuração e o fato de não ser necessário um servidor específico de autenticação. A desvantagem é que não se pode identificar fácilmente o usuário.

A seguir são apresentadas apenas as telas que são diferentes das apresentadas no método anterior (8.1).

Desabilitar o XAUTH na Fase 1:

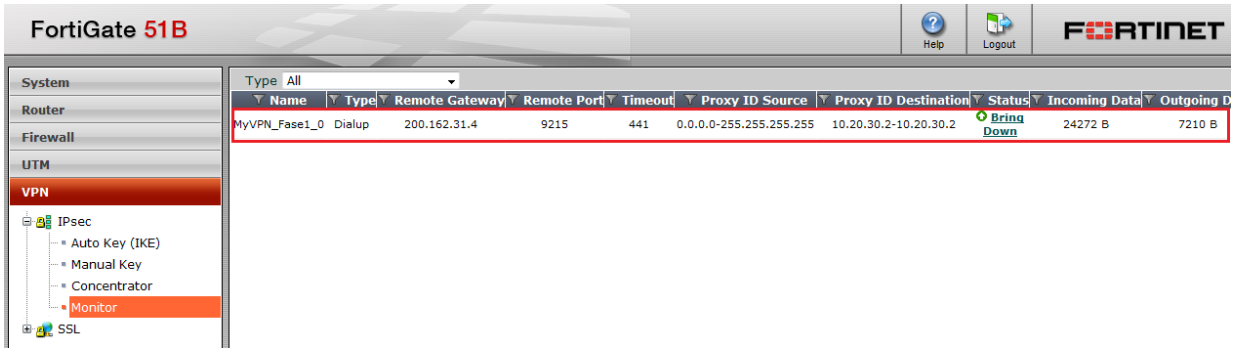


Desabilitar o check box eXtended Authentication no Forticlient:



Após estas configurações o Forticlient não mais requisitará o user name e password para estabelecer a VPN.

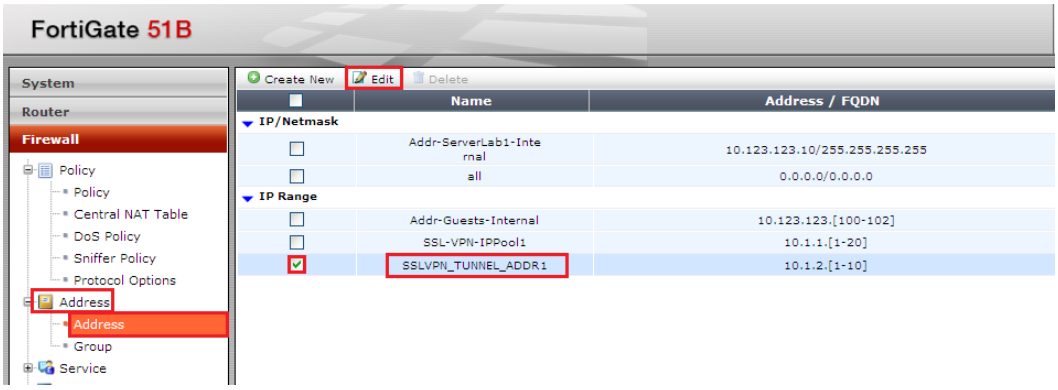
9.3 Monitoração dos Acessos à VPN IPSec

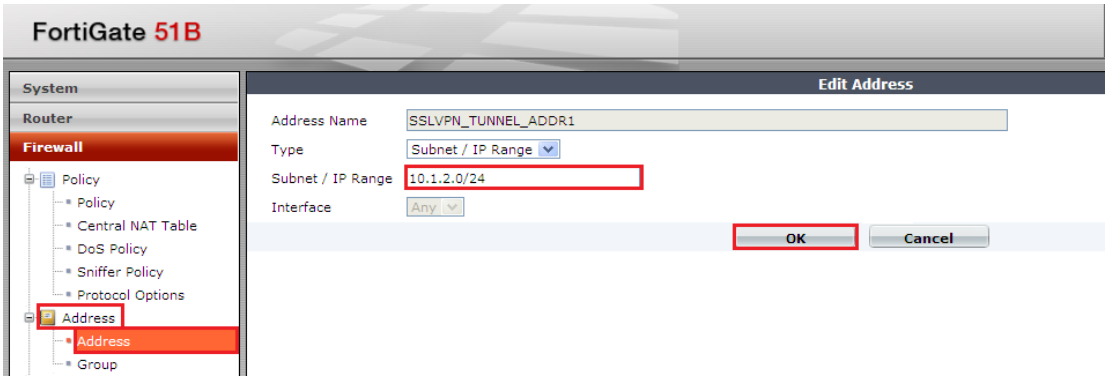


10 VPN SSL - Client-to-Site

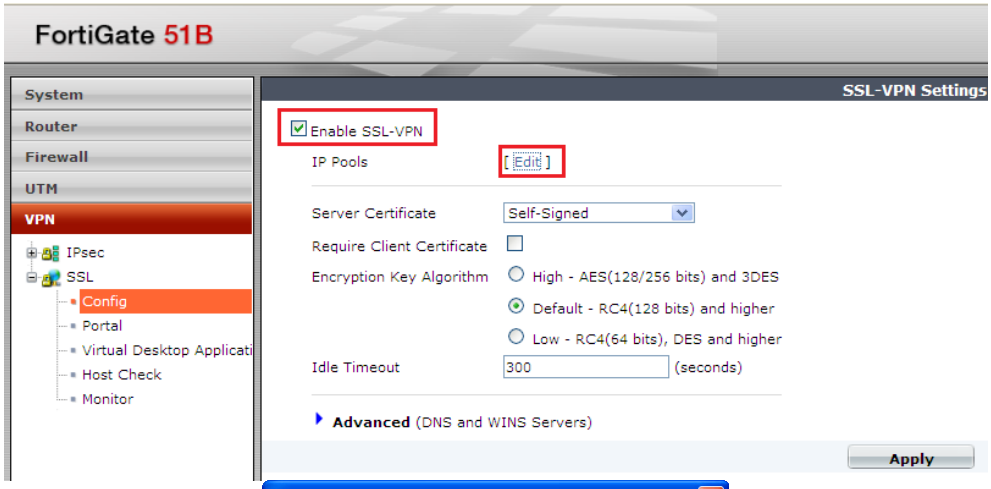
10.1 Acesso no Modo Web

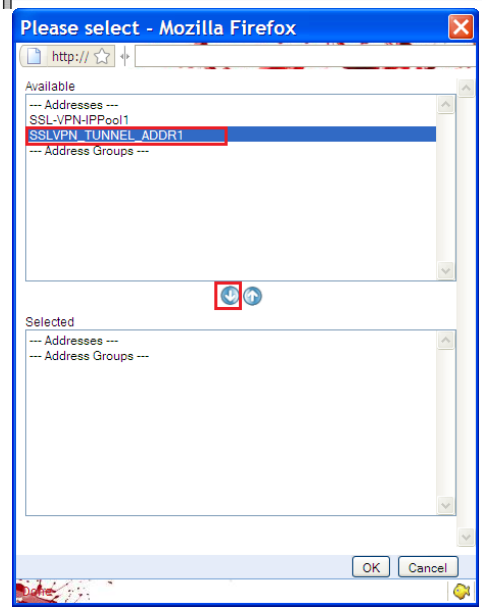
10.1.1 Editar o Address Range SSLVPN_TUNNEL_ADDR1

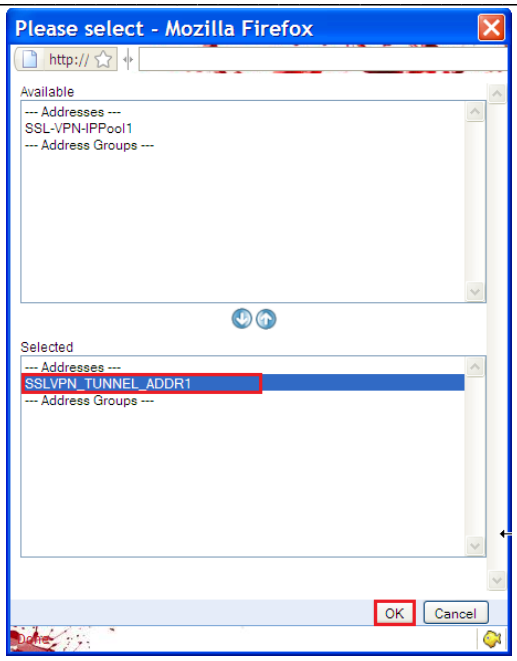


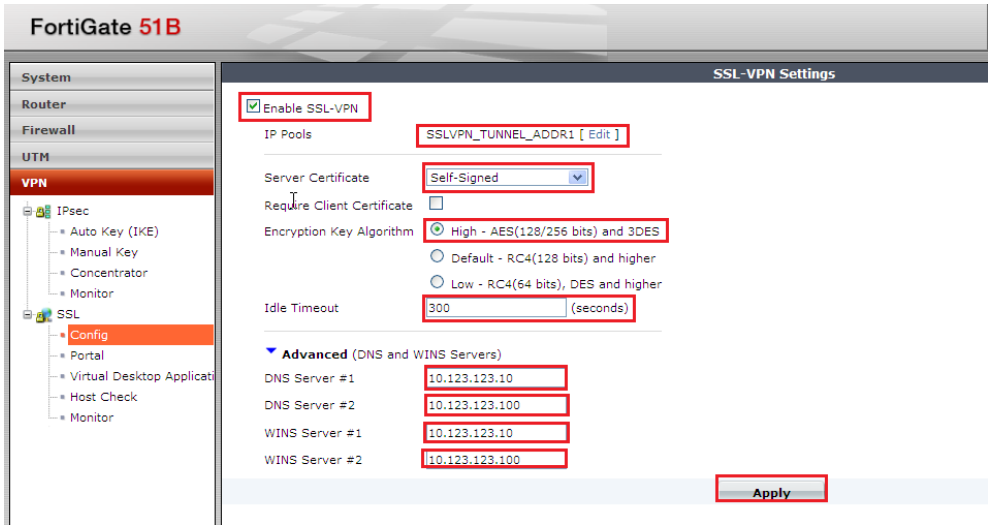


10.1.2 Habilitar SSL

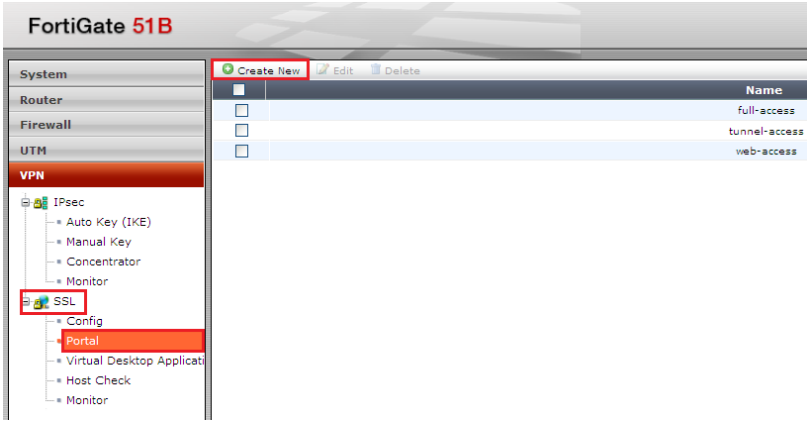


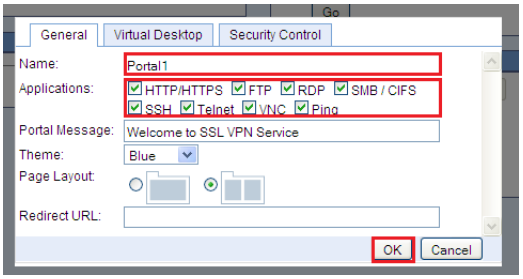


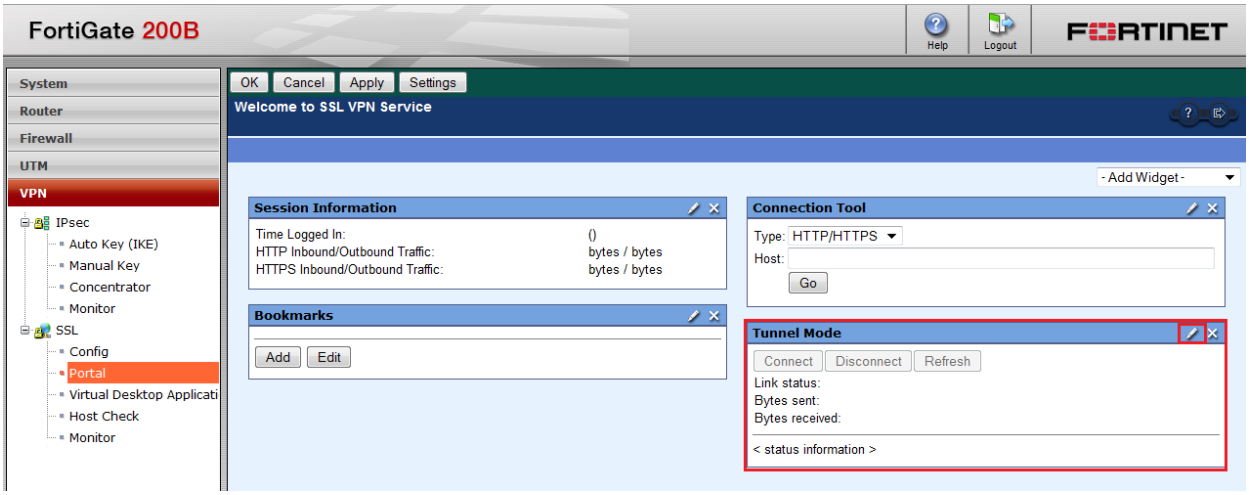


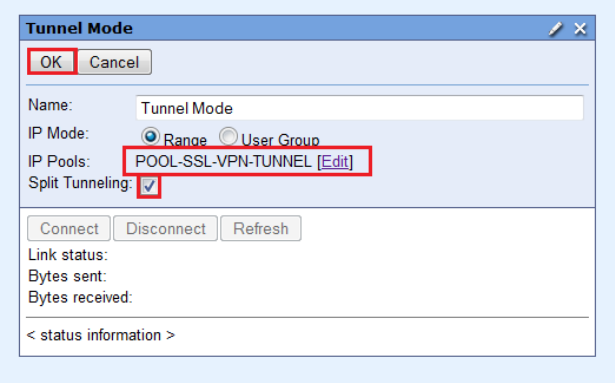


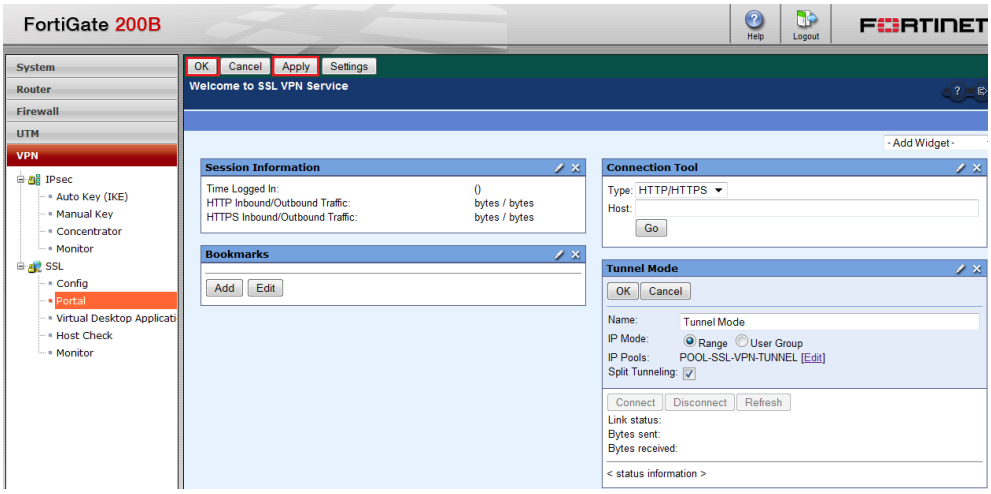
10.1.3 Criar Portal


FortiGate 51B
System
Router
Firewall
UTM
VPN
IPsec
Auto Key (IKE)
Manual Key
Concentrator
Monitor
SSL
Config
Portal
Virtual Desktop Applicati
Host Check
Monitor
Create New
Edit
Delete
Name
full-access
tunnel-access
web-access

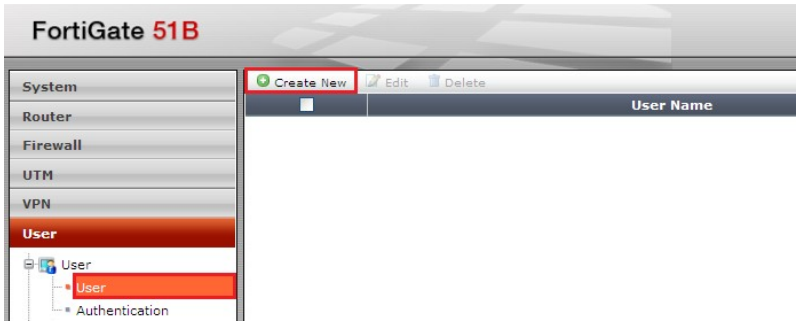

Go
General
Virtual Desktop
Security Control
Name:
Portal1
Applications:
HTTP/HTTPS
FTP
RDP
SMB / CIFS
SSH
Telnet
VNC
Ping
Portal Message:
Welcome to SSL VPN Service
Theme:
Blue
Page Layout:
Redirect URL:
OK
Cancel

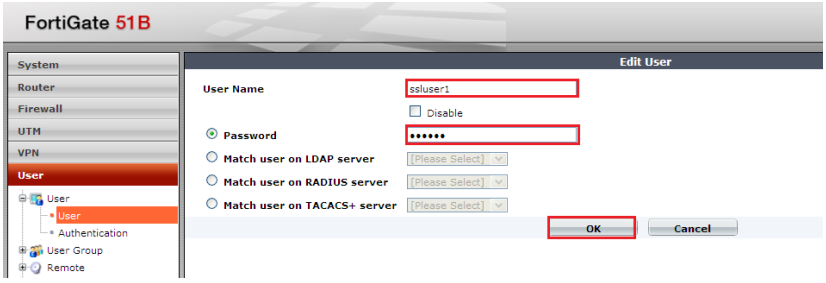

FortiGate 200B
Help
Logout
FORTINET
System
Router
Firewall
UTM
VPN
IPsec
Auto Key (IKE)
Manual Key
Concentrator
Monitor
SSL
Config
Portal
Virtual Desktop Applicati
Host Check
Monitor
OK
Cancel
Apply
Settings
Welcome to SSL VPN Service
- Add Widget -
Session Information
Time Logged In:
HTTP Inbound/Outbound Traffic:
HTTPS Inbound/Outbound Traffic:
bytes / bytes
bytes / bytes
Connection Tool
Type:
HTTP/HTTPS
Host:
Go
Bookmarks
Add
Edit
Tunnel Mode
Connect
Disconnect
Refresh
Link status:
Bytes sent:
Bytes received:
< status information >

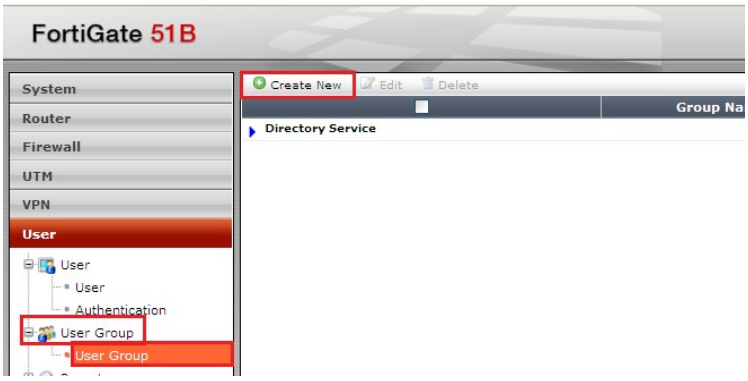


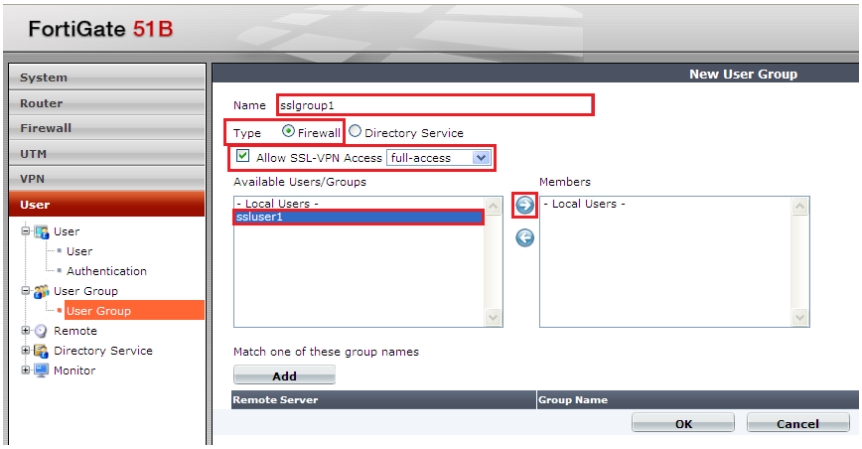


10.1.4 Criar conta e grupo para os usuários da SSL VPN.

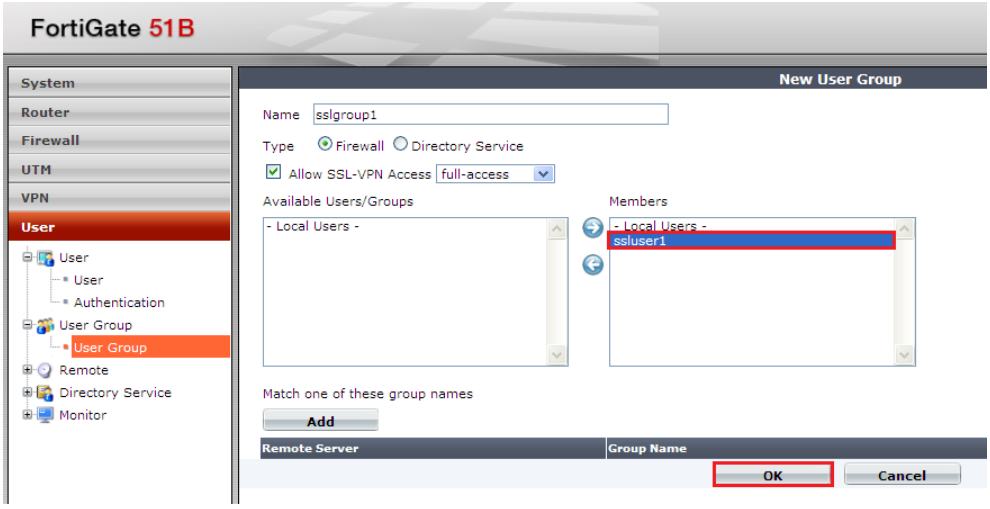




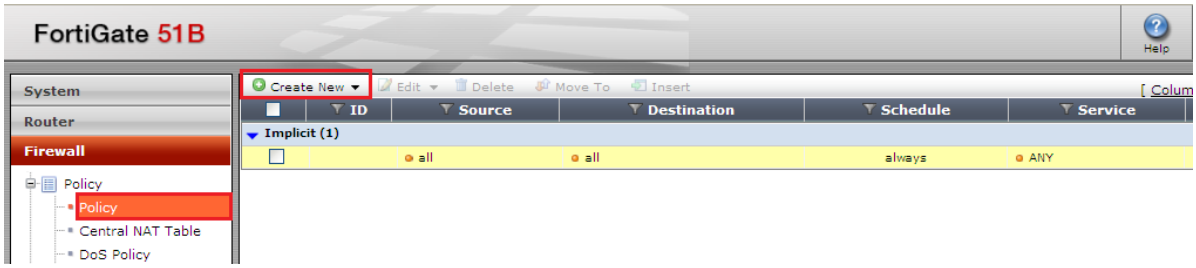


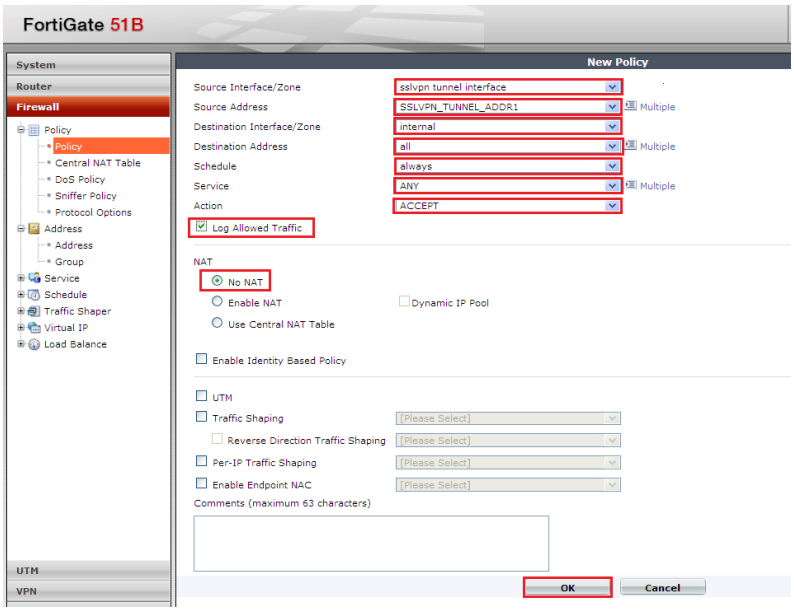


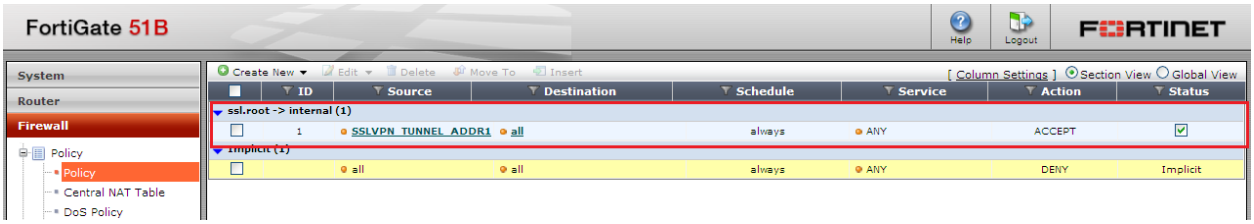
*Obs: A opção "Allow SSL-VPN = full-access" permitirá que os usuários deste grupo acessem a VPN SSL tanto no modo web como túnel.

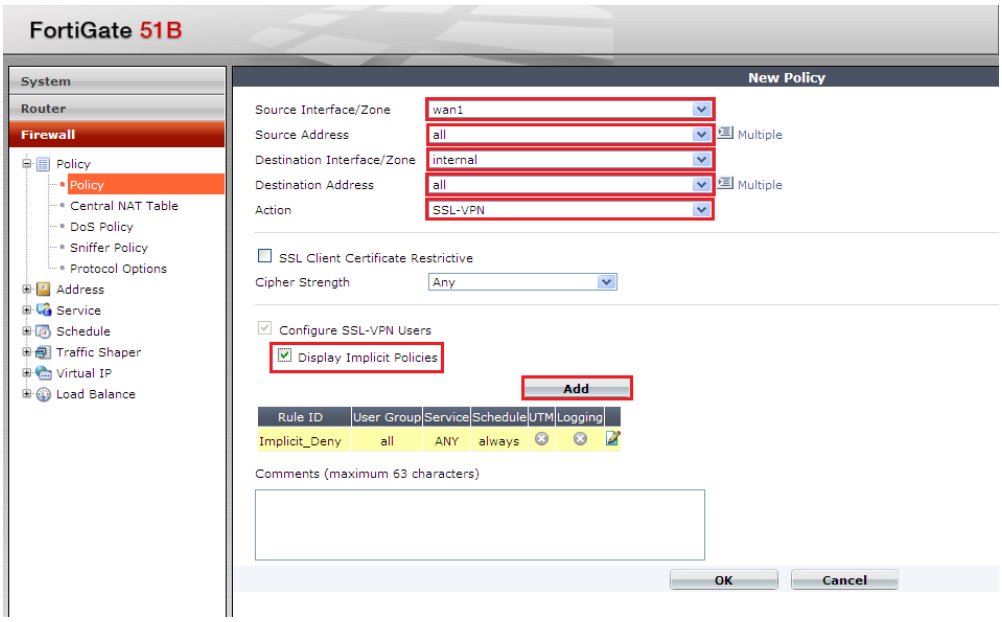


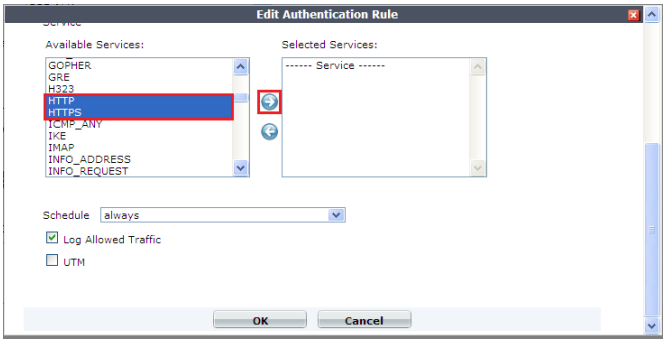
10.1.5 Criar regras para permitir o acesso externo à VPN SSL

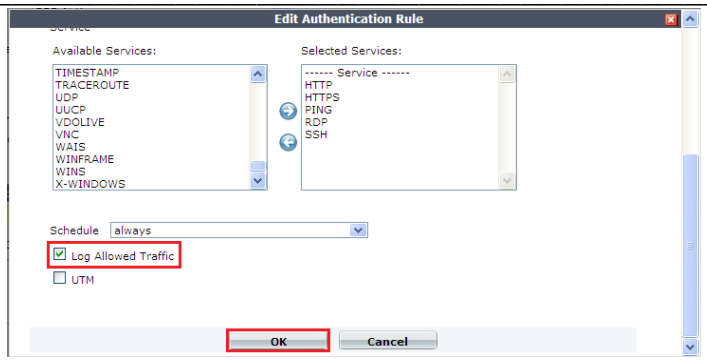


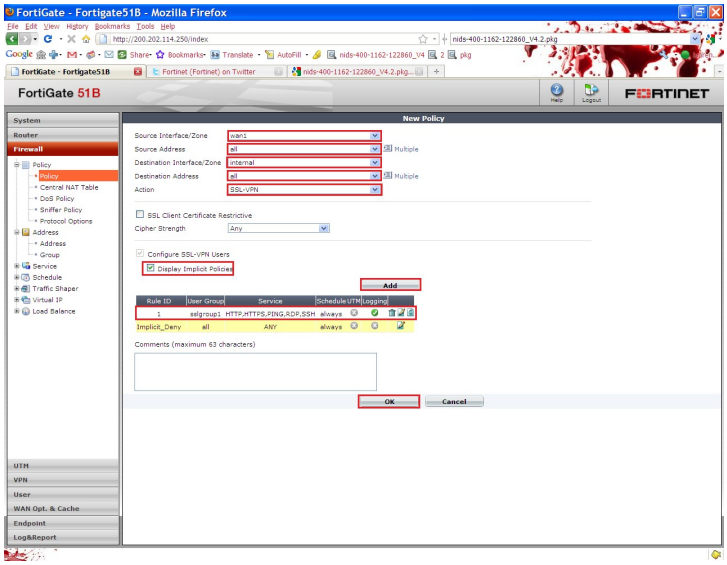


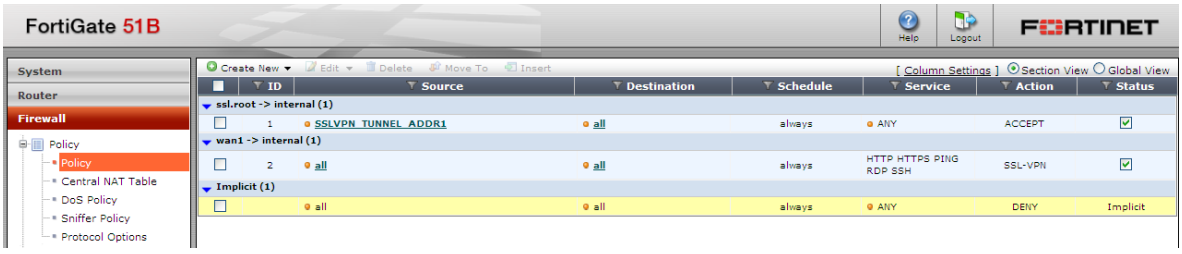

FortiGate 51B
Help
Logout
FORTINET
System
Router
Firewall
Policy
Policy
Central NAT Table
DoS Policy
Create New
Edit
Delete
Move To
Insert
[Column Settings]
Section View
Global View
ID
Source
Destination
Schedule
Service
Action
Status
ssl.root -> internal (1)
1
SSLVPN_TUNNEL_ADDR1
all
always
ANY
ACCEPT
Implicit (1)
all
all
always
ANY
DENY
Implicit


FortiGate 51B
System
Router
Firewall
Policy
Policy
Central NAT Table
DoS Policy
Sniffer Policy
Protocol Options
Address
Service
Schedule
Traffic Shaper
Virtual IP
Load Balance
New Policy
Source Interface/Zone
wan1
Source Address
all
Multiple
Destination Interface/Zone
internal
Destination Address
all
Multiple
Action
SSL-VPN
SSL Client Certificate Restrictive
Cipher Strength
Any
Configure SSL-VPN Users
Display Implicit Policies
Add
Rule ID
User Group
Service
Schedule
UTM
Logging
Implicit_Deny
all
ANY
always
Comments (maximum 63 characters)
OK
Cancel


Edit Authentication Rule
Available Services:
GOPHER
GRE
H323
HTTP
HTTPS
ICMP_ANY
IKE
IMAP
INFO_ADDRESS
INFO_REQUEST
Selected Services:
------ Service ------
Schedule
always
Log Allowed Traffic
UTM
OK
Cancel

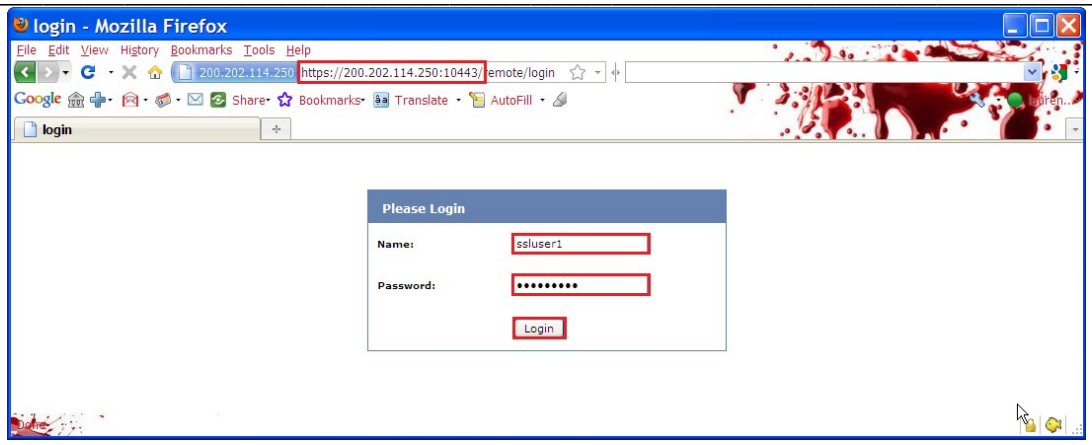


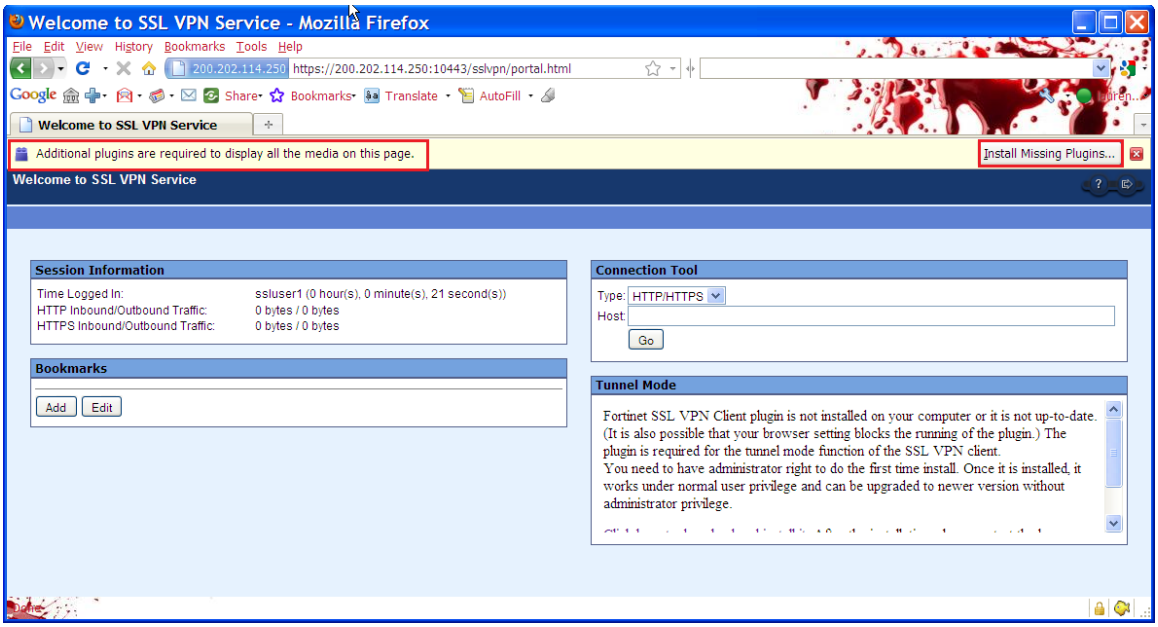




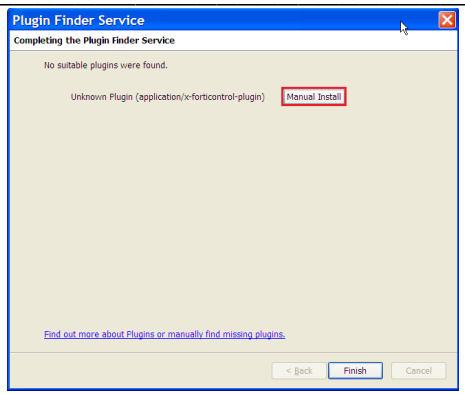
10.1.6 Acessar a VPN através do browser

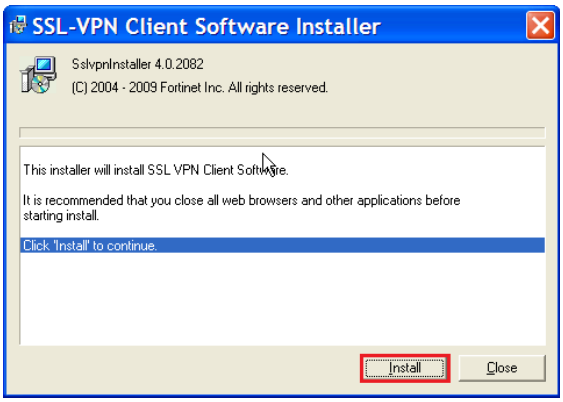
https://gateway_address:10443

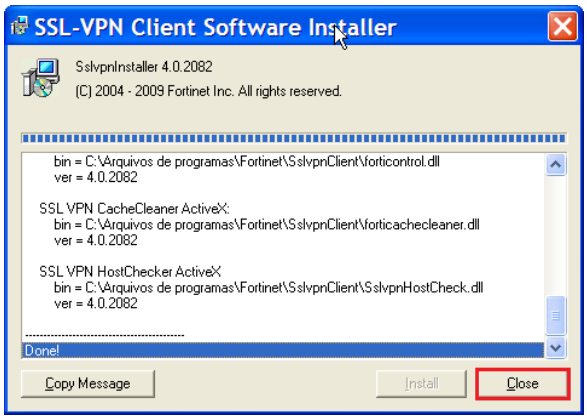




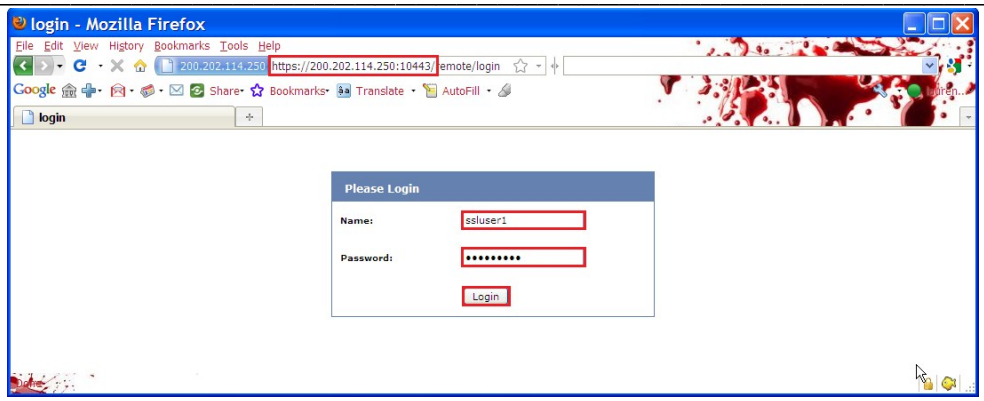
Fazer download e instalar manualmente (no caso do Firefox) o plugin.

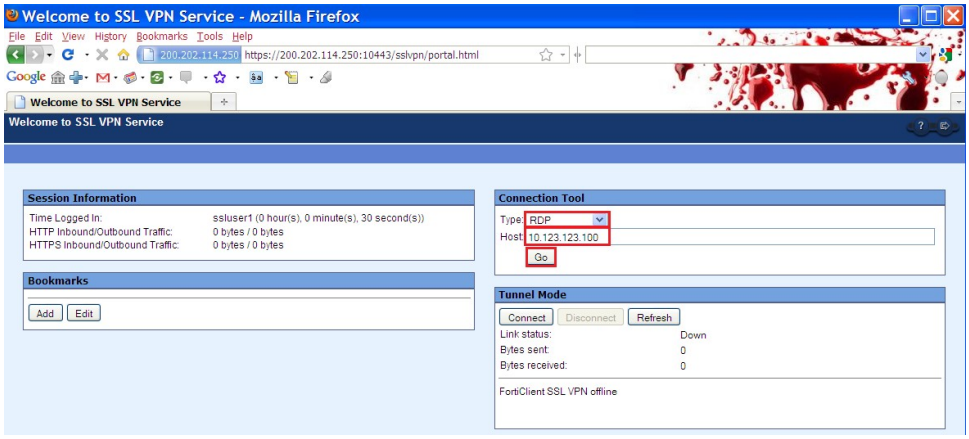


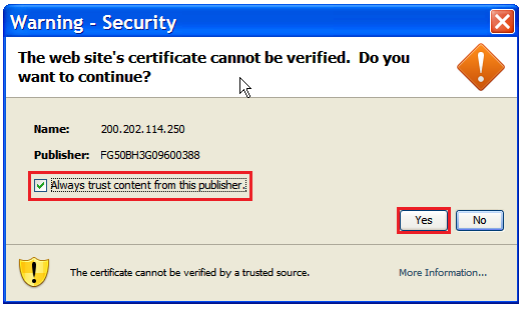


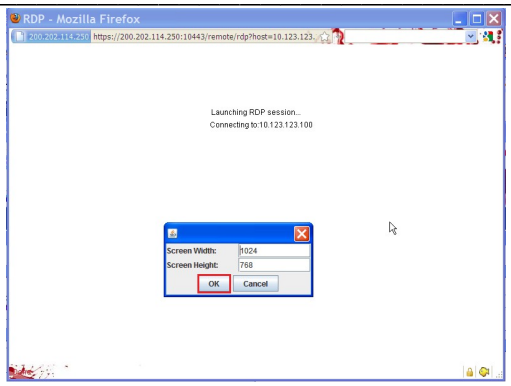


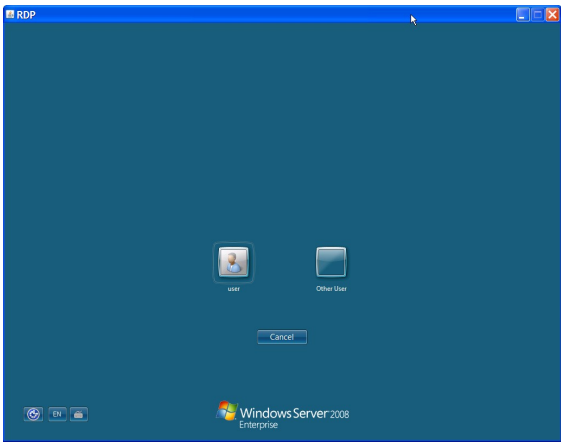
10.1.7 Exemplo de Acesso RDP

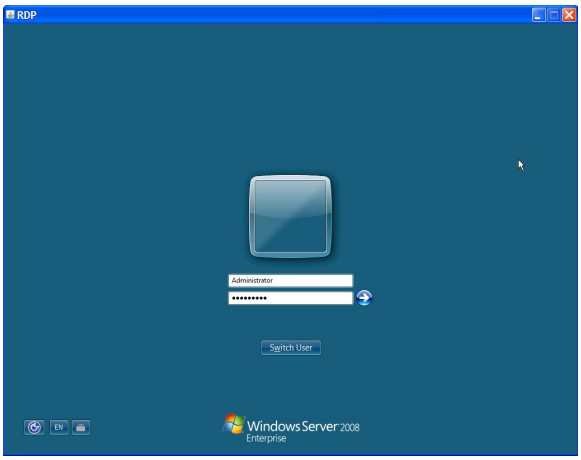

login - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://200.202.114.250:10443/remote/login
login
Please Login
Name:
ssluser1
Password:
Login

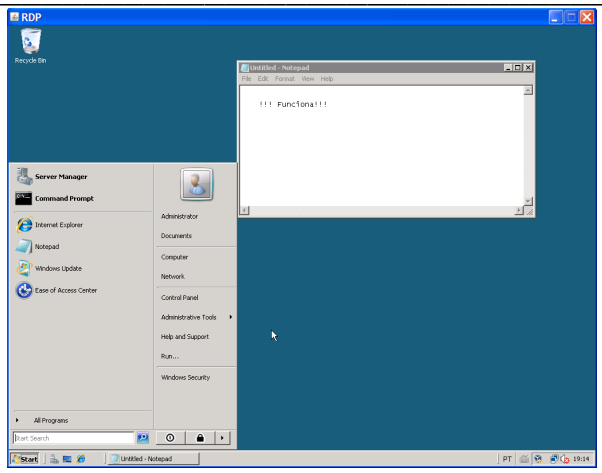

Welcome to SSL VPN Service - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://200.202.114.250:10443/sslvpn/portal.html
Welcome to SSL VPN Service
Welcome to SSL VPN Service
Session Information
Time Logged In: ssluser1 (0 hour(s), 0 minute(s), 30 second(s))
HTTP Inbound/Outbound Traffic: 0 bytes / 0 bytes
HTTPS Inbound/Outbound Traffic: 0 bytes / 0 bytes
Bookmarks
Add
Edit
Connection Tool
Type: RDP
Host: 10.123.123.100
Go
Tunnel Mode
Connect
Disconnect
Refresh
Link status: Down
Bytes sent: 0
Bytes received: 0
FortiClient SSL VPN offline


Warning - Security
The web site's certificate cannot be verified. Do you want to continue?
Name: 200.202.114.250
Publisher: FG50BH3G09600388
Always trust content from this publisher.
Yes
No
The certificate cannot be verified by a trusted source.
More Information...

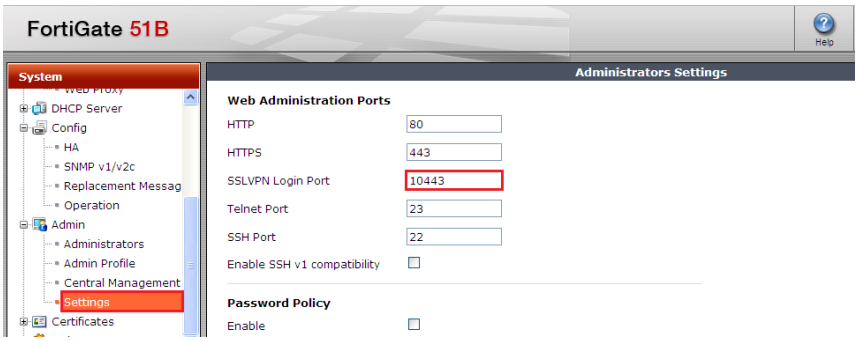

RDP - Mozilla Firefox
https://200.202.114.250:10443/remote/rdp?host=10.123.123.
Launching RDP session...
Connecting to:10.123.123.100
Screen Width:
1024
Screen Height:
768
OK
Cancel


RDP
user
Other User
Cancel
Windows Server 2008
Enterprise

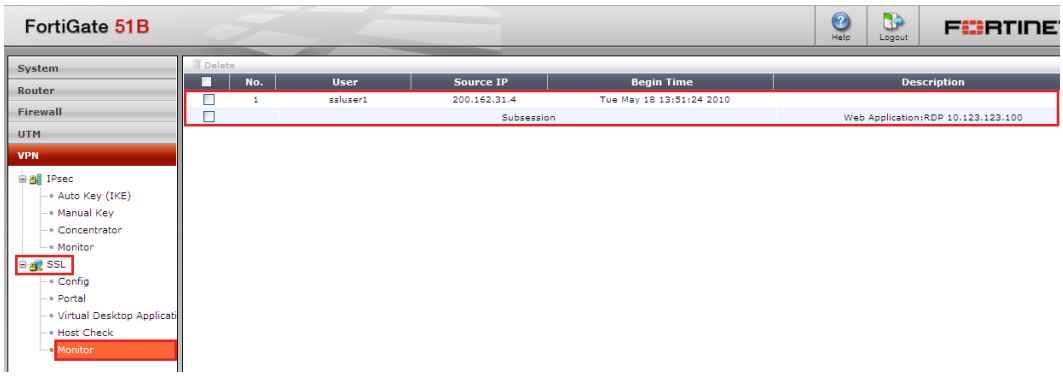

RDP
Administrator
Switch User
Windows Server 2008
Enterprise



10.1.8 Configuração Opcional: Alterar Porta de Acesso à SSL VPN

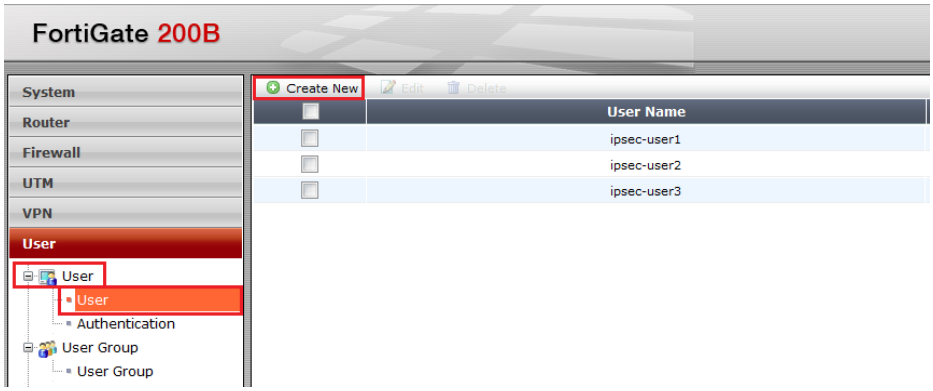


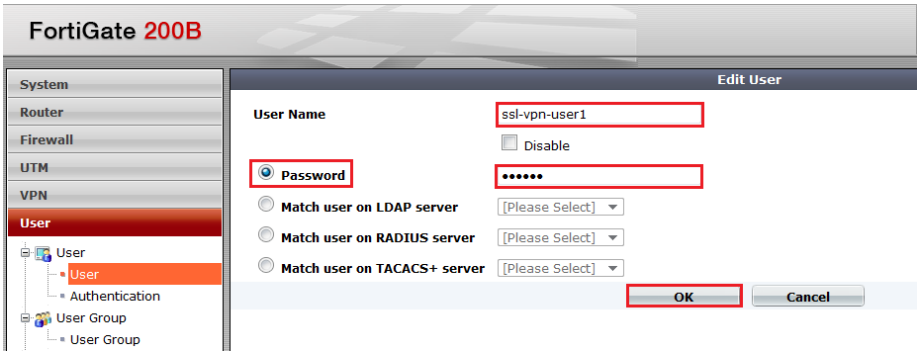
10.1.9 Monitoração dos Acessos

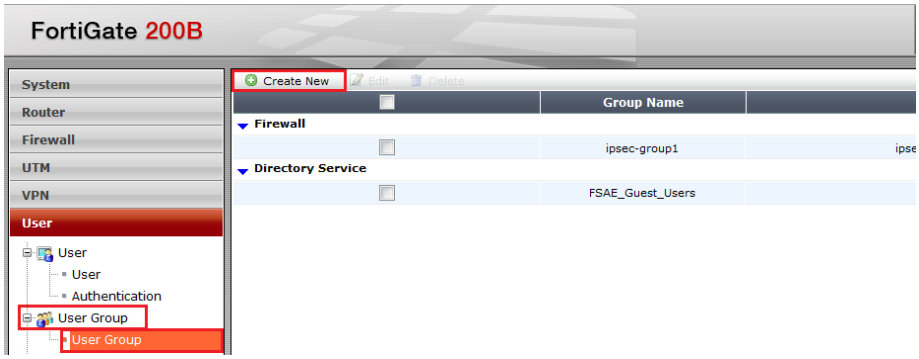


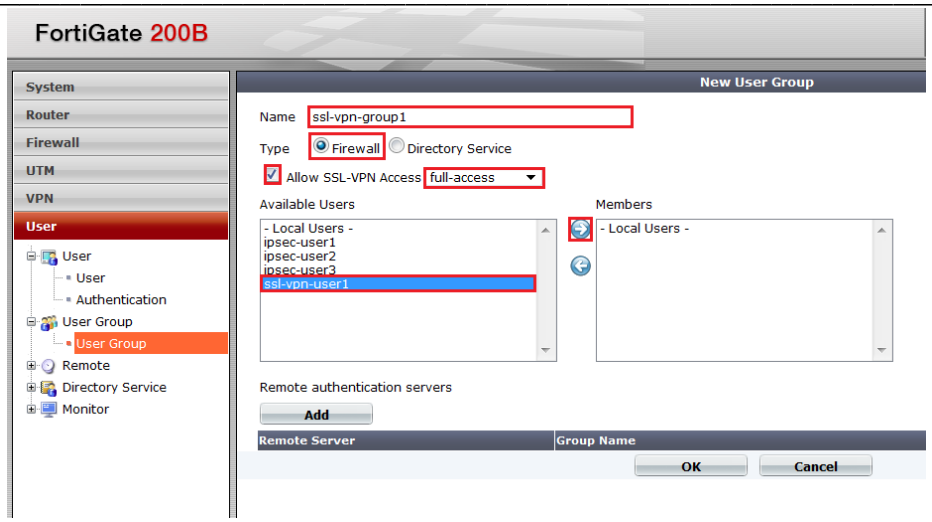
10.2 Acesso no Modo Túnel

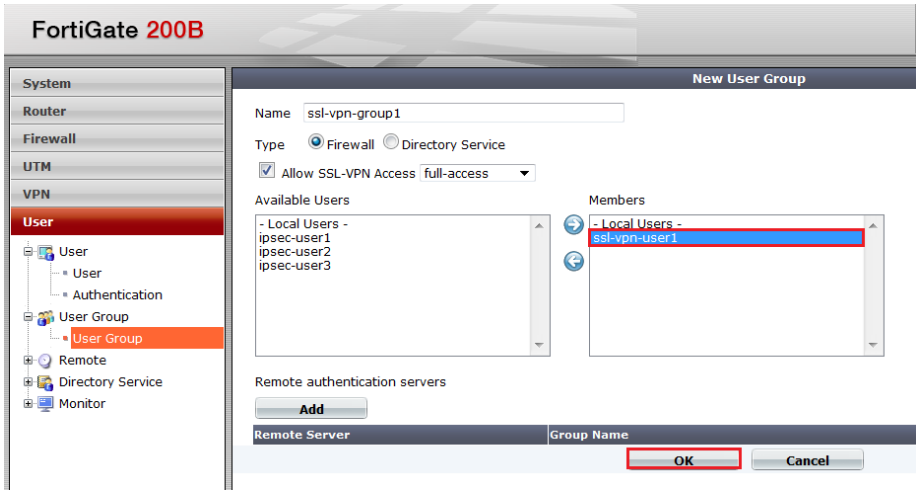
1. Criar usuários e grupo da SSL VPN



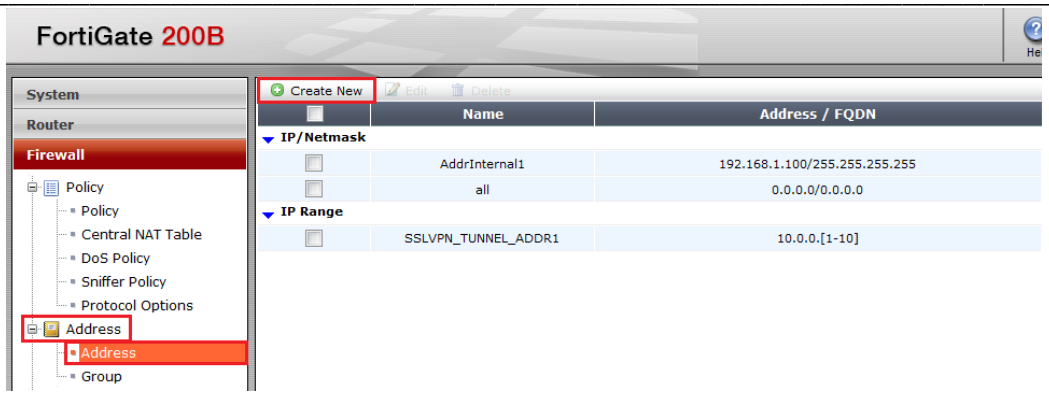


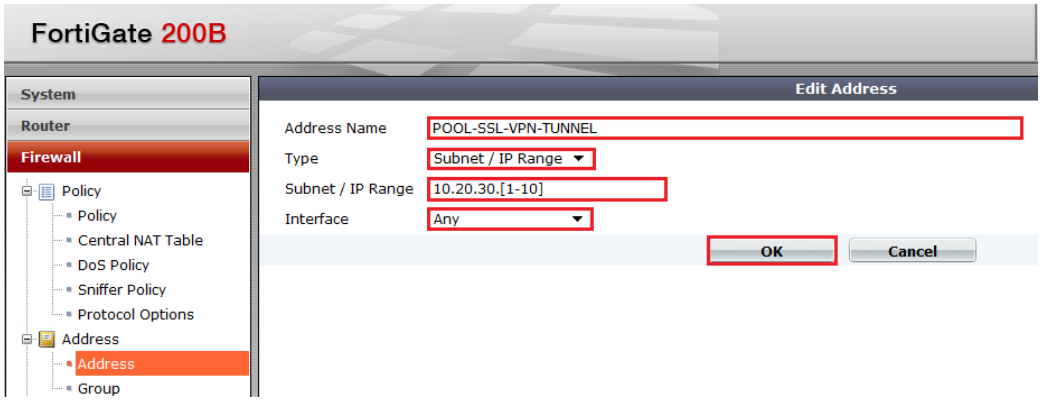




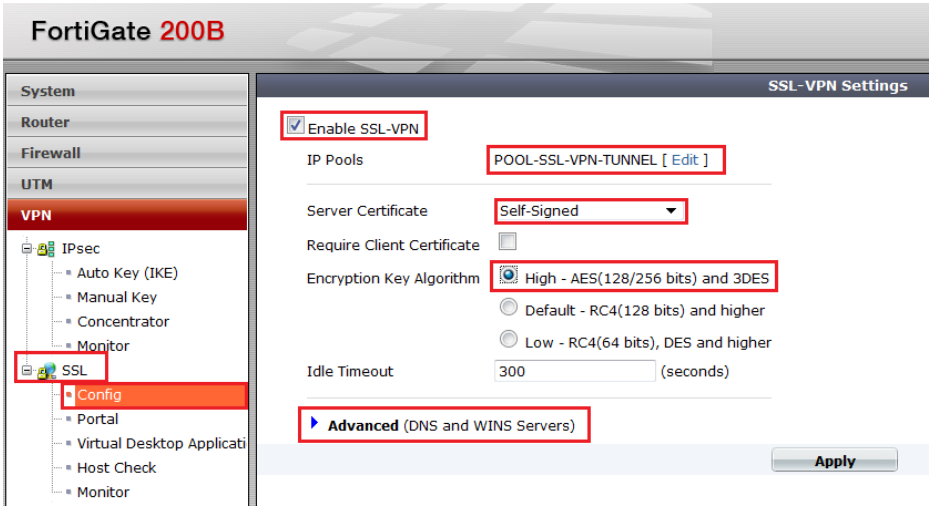


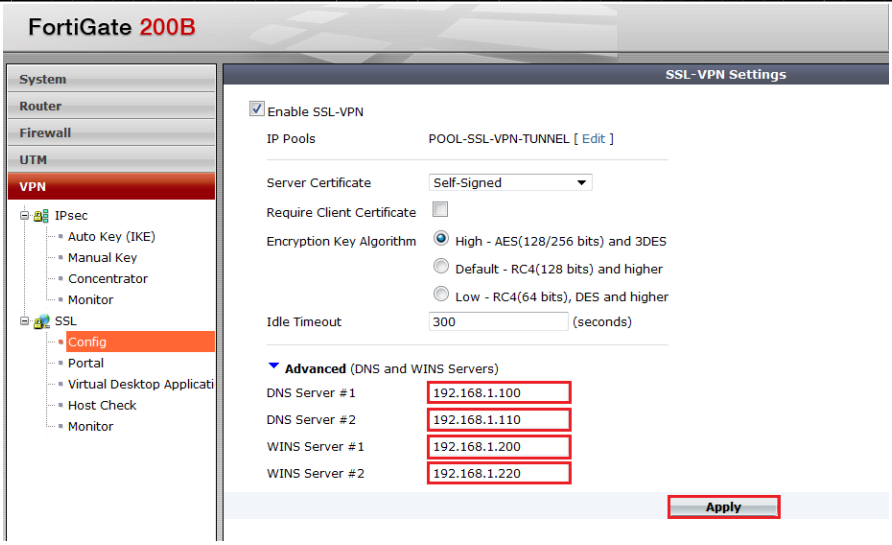
2. Criar um pool de endereços IP que serão usados para os clientes da SSL VPN no modo túnel. Ao se conectar à VPN os clientes receberão um endereço deste pool.



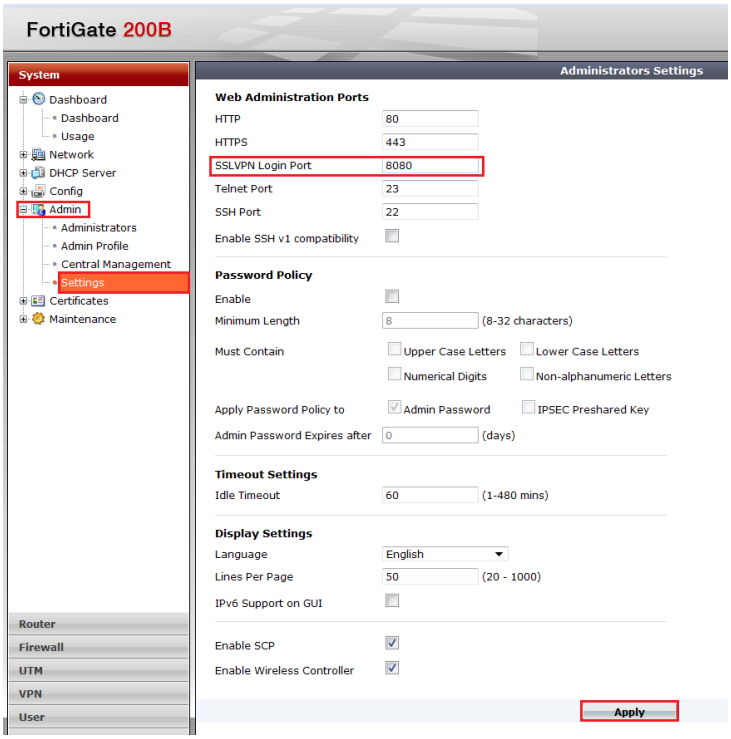


3. Habilitar a VPN. No campo IP Pools deve-se selecionar o endereço definido previamente. Definir endereços dos servidores DNS e WINS se necessário.

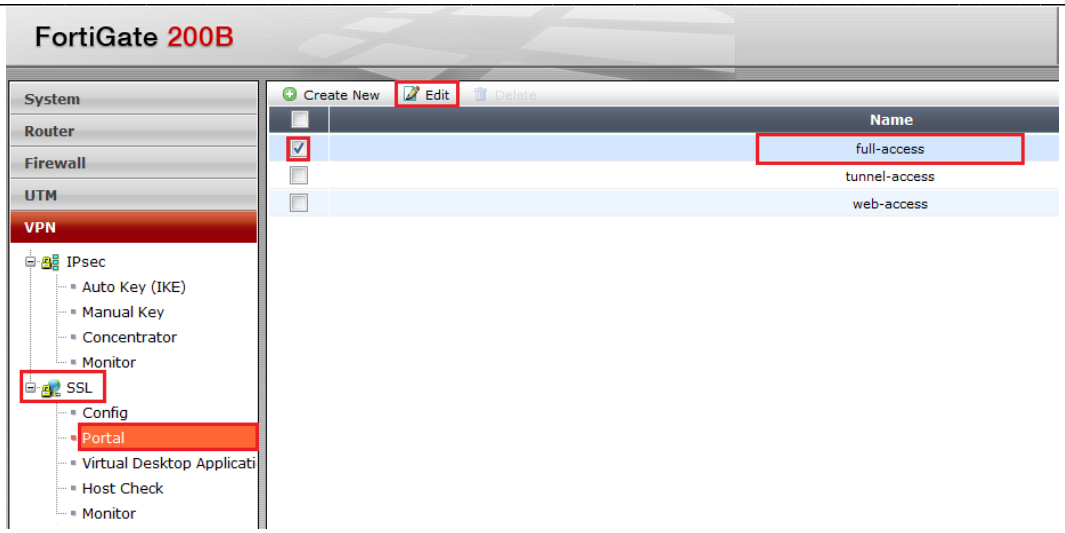




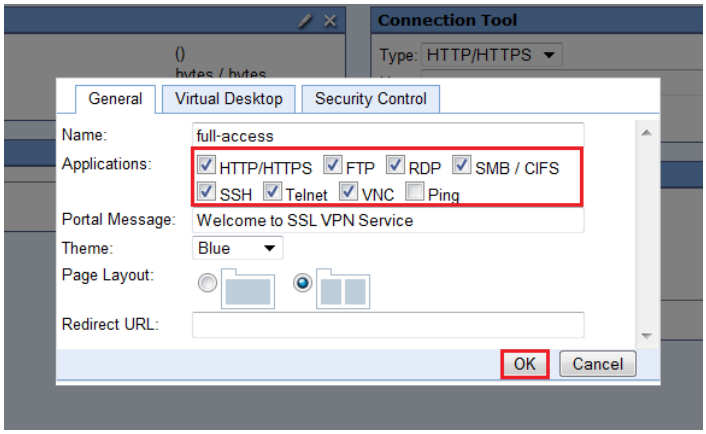
4. Alterar a porta a ser utilizada na VPN SSL. Por default esta porta é TCP/10443. Caso necessário ela pode ser alterada. No exemplo abaixo a porta foi alterada para TCP/8080.



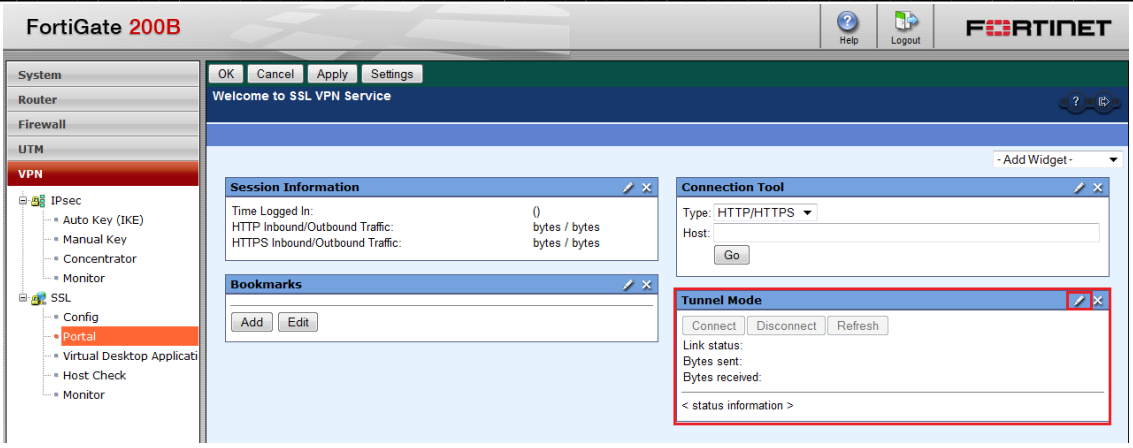
5. Editar o portal “full-access” (especificado na configuração do grupo).

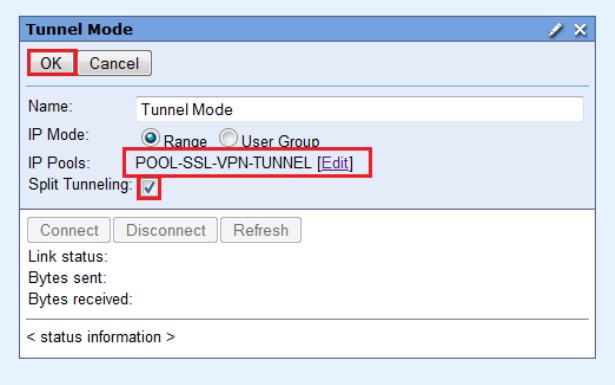


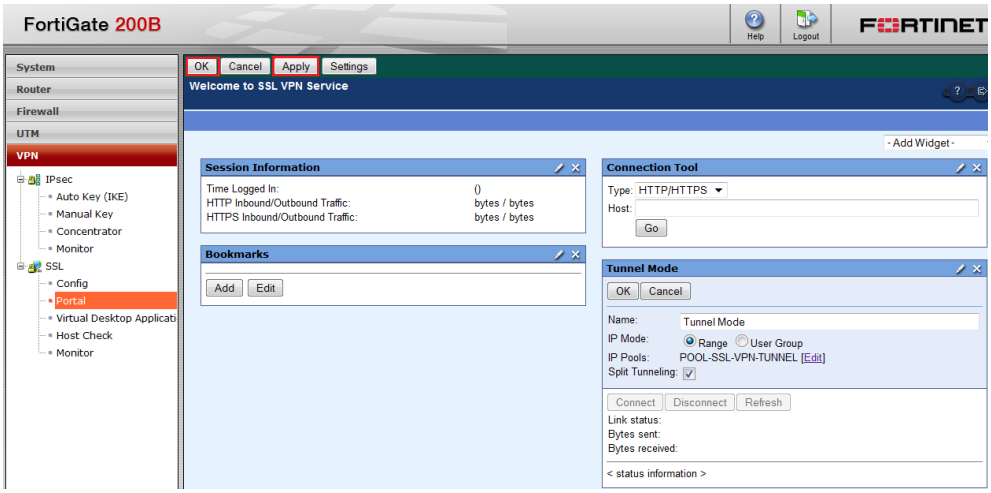
6. Habilitar os serviços a serem permitidos na VPN Web Mode.



7. Definir o pool de endereços distribuídos aos clientes e habilitar o Split Tunneling no Tunnel Mode.

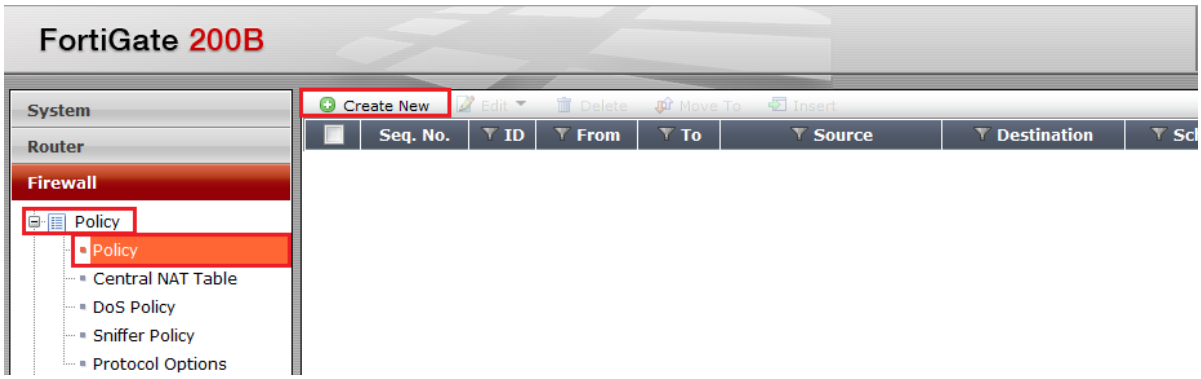

FortiGate 200B
Help
Logout
FORTINET
System
Router
Firewall
UTM
VPN
IPsec
Auto Key (IKE)
Manual Key
Concentrator
Monitor
SSL
Config
Portal
Virtual Desktop Applicati
Host Check
Monitor
OK
Cancel
Apply
Settings
Welcome to SSL VPN Service
- Add Widget -
Session Information
Time Logged In:
HTTP Inbound/Outbound Traffic:
HTTPS Inbound/Outbound Traffic:
bytes / bytes
bytes / bytes
Connection Tool
Type: HTTP/HTTPS
Host:
Go
Bookmarks
Add
Edit
Tunnel Mode
Connect
Disconnect
Refresh
Link status:
Bytes sent:
Bytes received:
< status information >


Tunnel Mode
OK
Cancel
Name:
Tunnel Mode
IP Mode:
Range
User Group
IP Pools:
POOL-SSL-VPN-TUNNEL [Edit]
Split Tunneling:
Connect
Disconnect
Refresh
Link status:
Bytes sent:
Bytes received:
< status information >


FortiGate 200B
Help
Logout
FORTINET
System
Router
Firewall
UTM
VPN
IPsec
Auto Key (IKE)
Manual Key
Concentrator
Monitor
SSL
Config
Portal
Virtual Desktop Applicati
Host Check
Monitor
OK
Cancel
Apply
Settings
Welcome to SSL VPN Service
- Add Widget -
Session Information
Time Logged In:
HTTP Inbound/Outbound Traffic:
HTTPS Inbound/Outbound Traffic:
bytes / bytes
bytes / bytes
Connection Tool
Type: HTTP/HTTPS
Host:
Go
Bookmarks
Add
Edit
Tunnel Mode
OK
Cancel
Name:
Tunnel Mode
IP Mode:
Range
User Group
IP Pools:
POOL-SSL-VPN-TUNNEL [Edit]
Split Tunneling:
Connect
Disconnect
Refresh
Link status:
Bytes sent:
Bytes received:
< status information >

8. Criar regras de firewall.

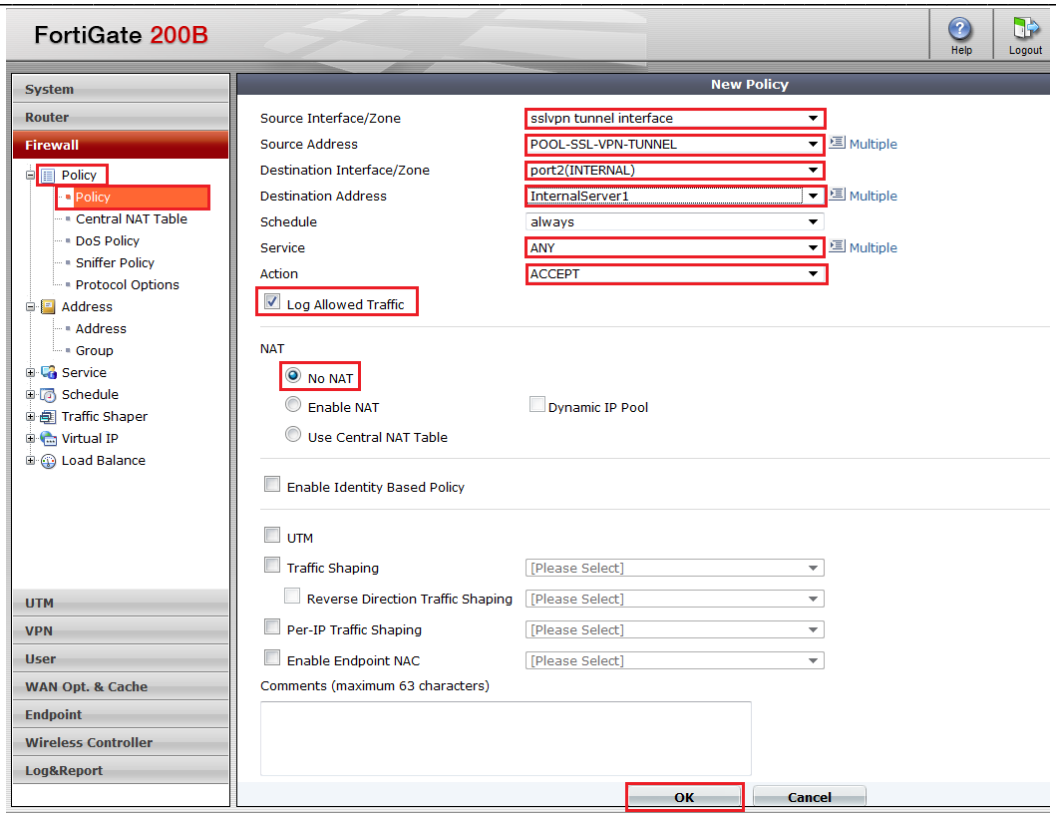
Os endereços a serem utilizados nas regras são apresentados abaixo:



Regra 1: Acesso dos clientes de VPN ao InternalServer1.

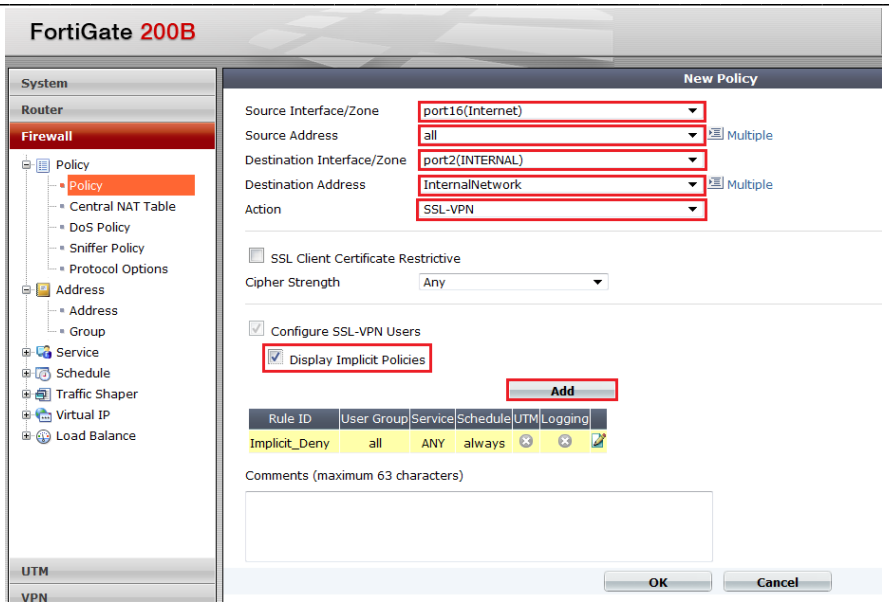
***Obs1**: No Destination Address deve-se evitar o uso do grupo “all”. Isto deve ser evitado pois as rotas inseridas nos clients são “aprendidas” através dos endereços de destino nas regras do firewall. Um regra com destino “all” fará com que todos os pacotes de dados enviados pelo client sejam enviados através do túnel!

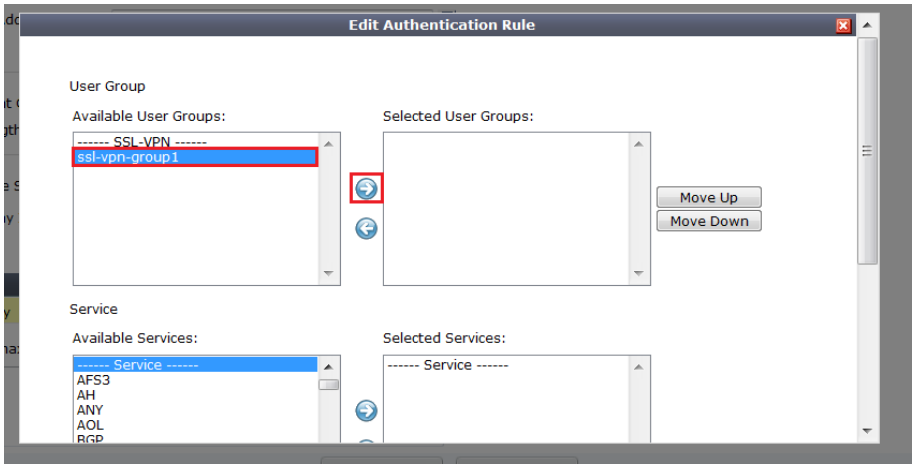
***Obs2**: A Source Interface que representa o túnel SSL (chamada “ssl tunnel interface” na tela abaixo) pode às vezes aparecer como “ssl.root”.

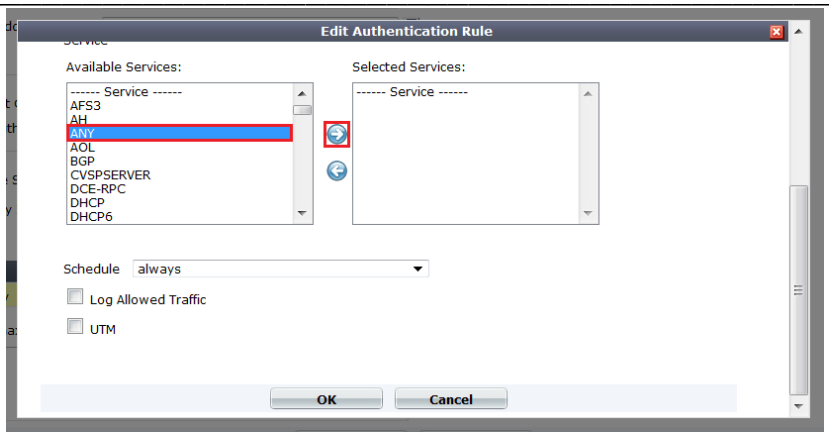


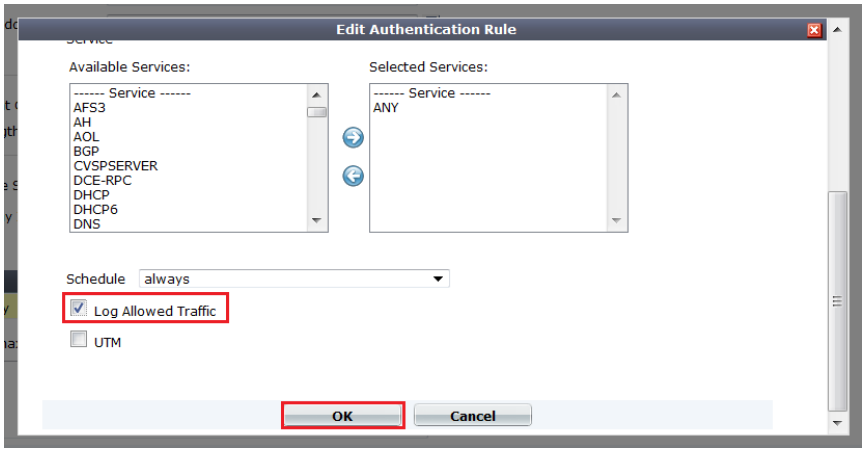
Regra 2: Estabelecimento da SSL VPN.

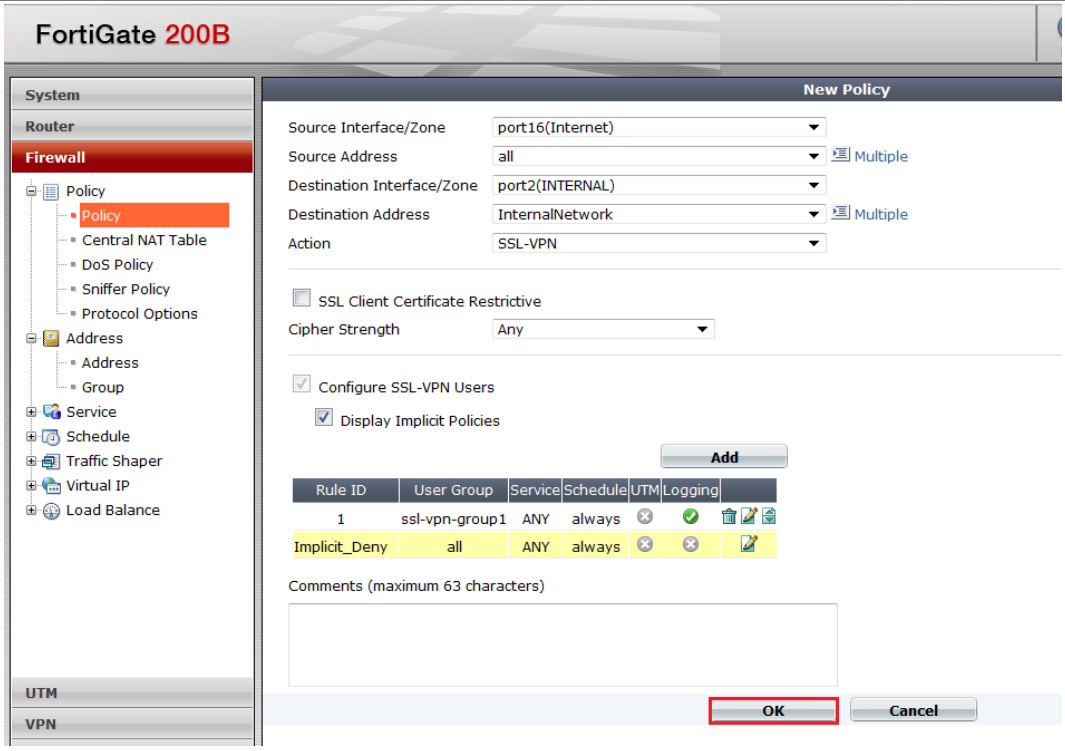
***Obs1**: No Destination Address deve-se evitar o uso do grupo “all”. Isto deve ser evitado pois as rotas inseridas nos clients são “aprendidas” através dos endereços de destino nas regras do firewall. Um regra com destino “all” fará com que todos os pacotes de dados enviados pelo client sejam enviados através do túnel!

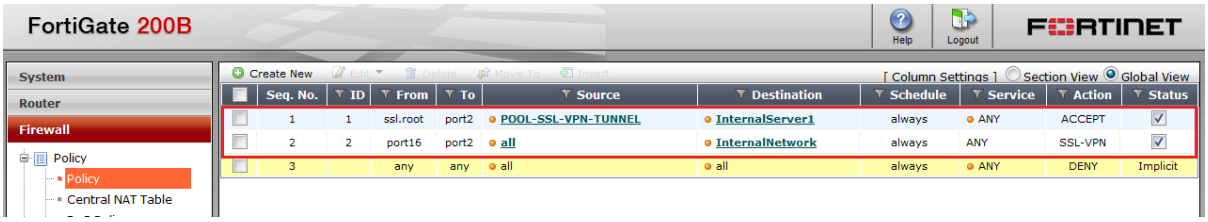

FortiGate 200B
System
Router
Firewall
Policy
Policy
Central NAT Table
DoS Policy
Sniffer Policy
Protocol Options
Address
Address
Group
Service
Schedule
Traffic Shaper
Virtual IP
Load Balance
UTM
VPN
New Policy
Source Interface/Zone
port16(Internet)
Source Address
all
Multiple
Destination Interface/Zone
port2(INTERNAL)
Destination Address
InternalNetwork
Multiple
Action
SSL-VPN
SSL Client Certificate Restrictive
Cipher Strength
Any
Configure SSL-VPN Users
Display Implicit Policies
Add
Rule ID
User Group
Service
Schedule
UTM
Logging
Implicit_Deny
all
ANY
always
Comments (maximum 63 characters)
OK
Cancel


Edit Authentication Rule
User Group
Available User Groups:
------ SSL-VPN ------
ssl-vpn-group1
Selected User Groups:
Move Up
Move Down
Service
Available Services:
------ Service ------
AFS3
AH
ANY
AOL
Selected Services:
------ Service ------

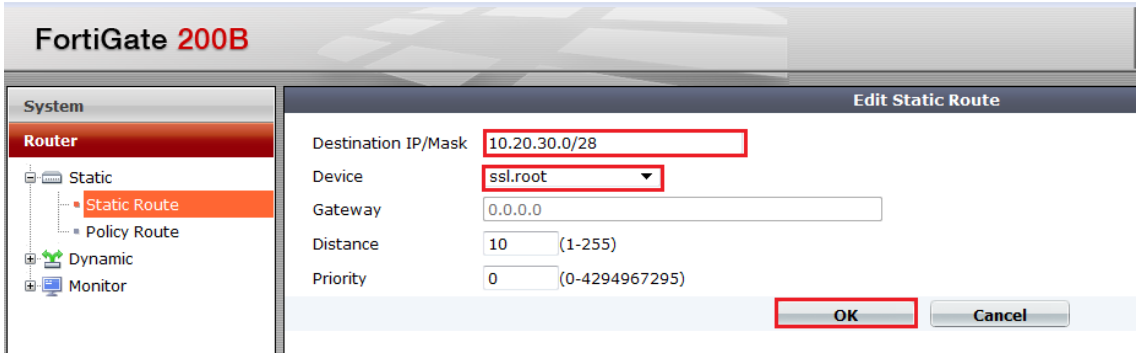

Edit Authentication Rule
Available Services:
Selected Services:
------ Service ------
AFS3
AH
ANY
AOL
BGP
CVSPSERVER
DCE-RPC
DHCP
DHCP6
------ Service ------
Schedule
always
Log Allowed Traffic
UTM
OK
Cancel


Edit Authentication Rule
Available Services:
Selected Services:
------ Service ------
AFS3
AH
AOL
BGP
CVSPSERVER
DCE-RPC
DHCP
DHCP6
DNS
------ Service ------
ANY
Schedule
always
Log Allowed Traffic
UTM
OK
Cancel

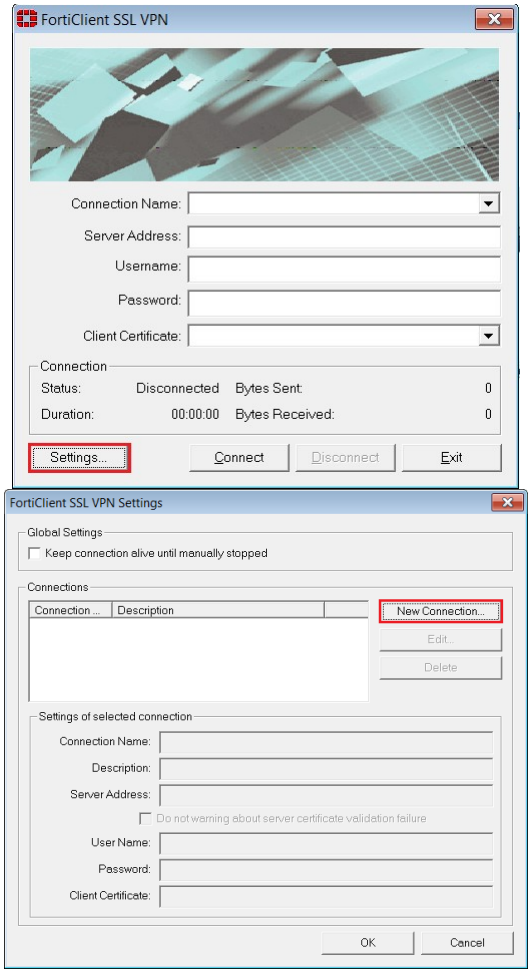


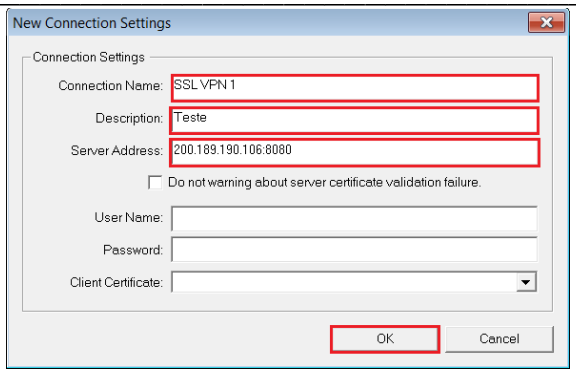


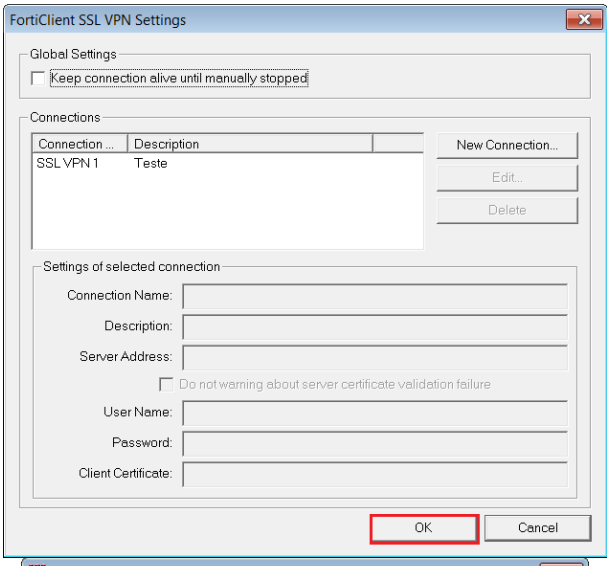
9. Criar rota estática para o túnel SSL. O endereço de rede a ser especificado é o do pool de endereços utilizados pelos clientes da VPN (POOL-SSL-VPN-TUNNEL).

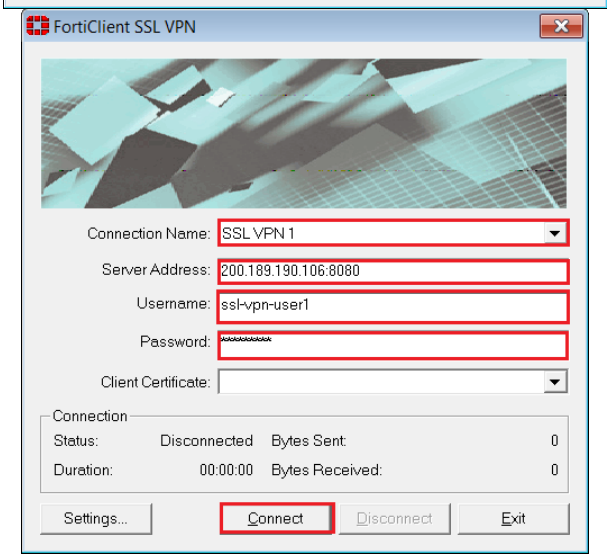


10. Configurar o client e conectar à VPN.

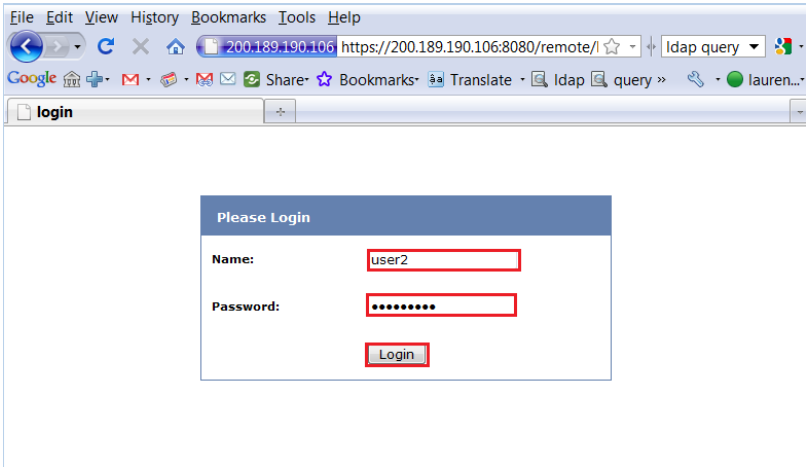



New Connection Settings
Connection Settings
Connection Name: SSL VPN 1
Description: Teste
Server Address: 200.189.190.106:8080
Do not warning about server certificate validation failure.
User Name:
Password:
Client Certificate:
OK
Cancel

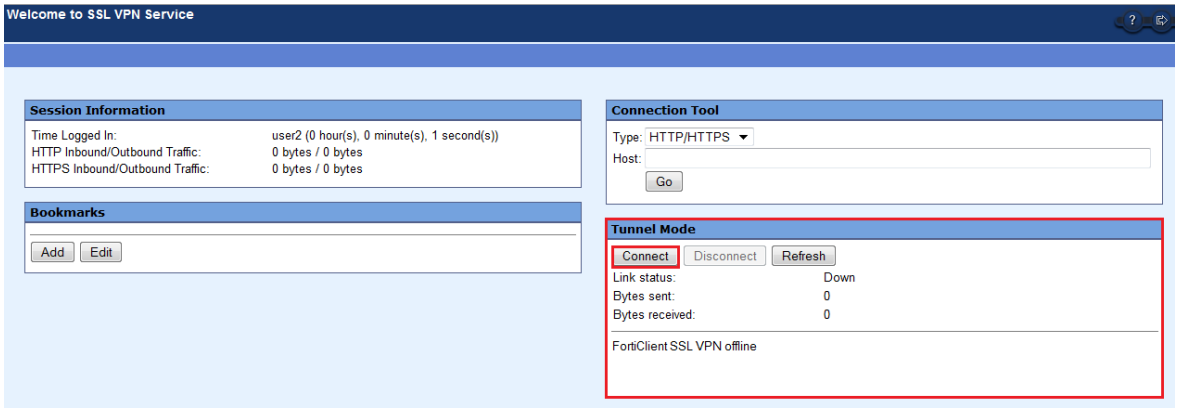

FortiClient SSL VPN Settings
Global Settings
Keep connection alive until manually stopped
Connections
Connection ...
Description
SSL VPN 1
Teste
New Connection...
Edit...
Delete
Settings of selected connection
Connection Name:
Description:
Server Address:
Do not warning about server certificate validation failure
User Name:
Password:
Client Certificate:
OK
Cancel


FortiClient SSL VPN
Connection Name: SSL VPN 1
Server Address: 200.189.190.106:8080
Username: ssl-vpn-user1
Password:
Client Certificate:
Connection
Status: Disconnected
Bytes Sent: 0
Duration: 00:00:00
Bytes Received: 0
Settings...
Connect
Disconnect
Exit

11. Forma alternativa de conexão à VPN no modo túnel. O client deve estar previamente instalado.
    Acessar o gateway através do browser e fazer o login.



12. Forma alternativa de conexão à VPN no modo túnel. O client deve estar previamente instalado.
    Acessar o gateway através do browser e fazer o login.



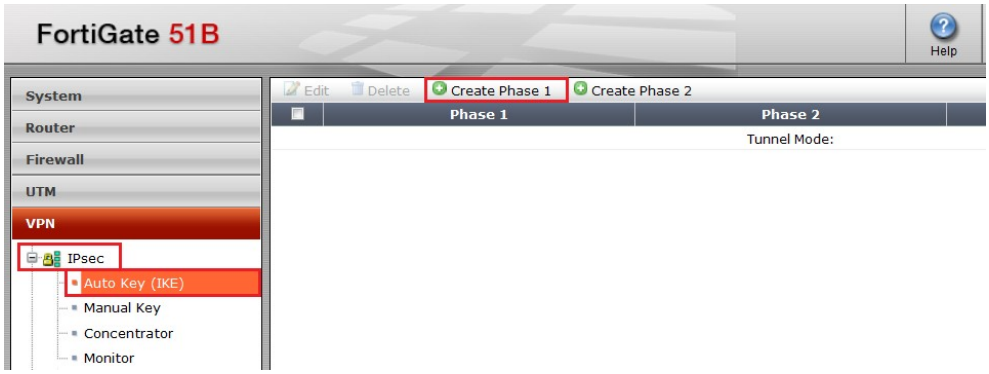
10.3 Monitoração de Acessos

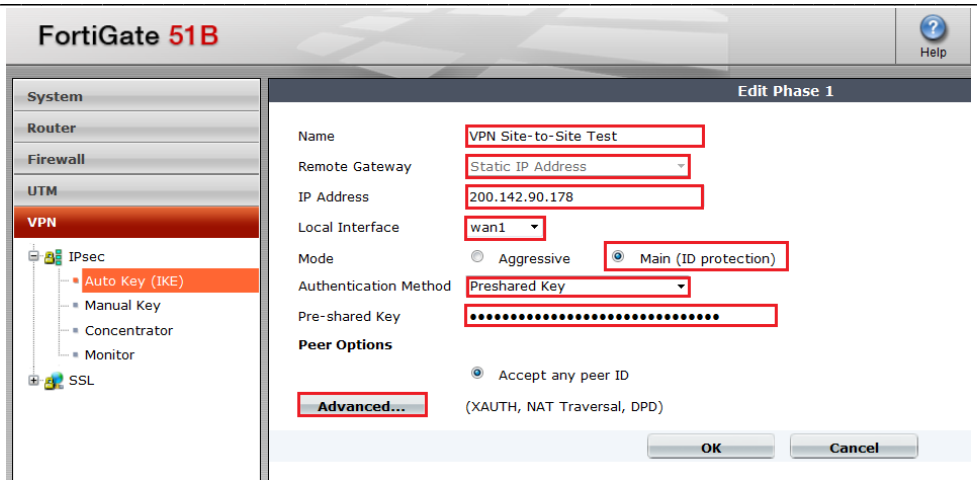
11 VPN IPSEC – Site-to-Site

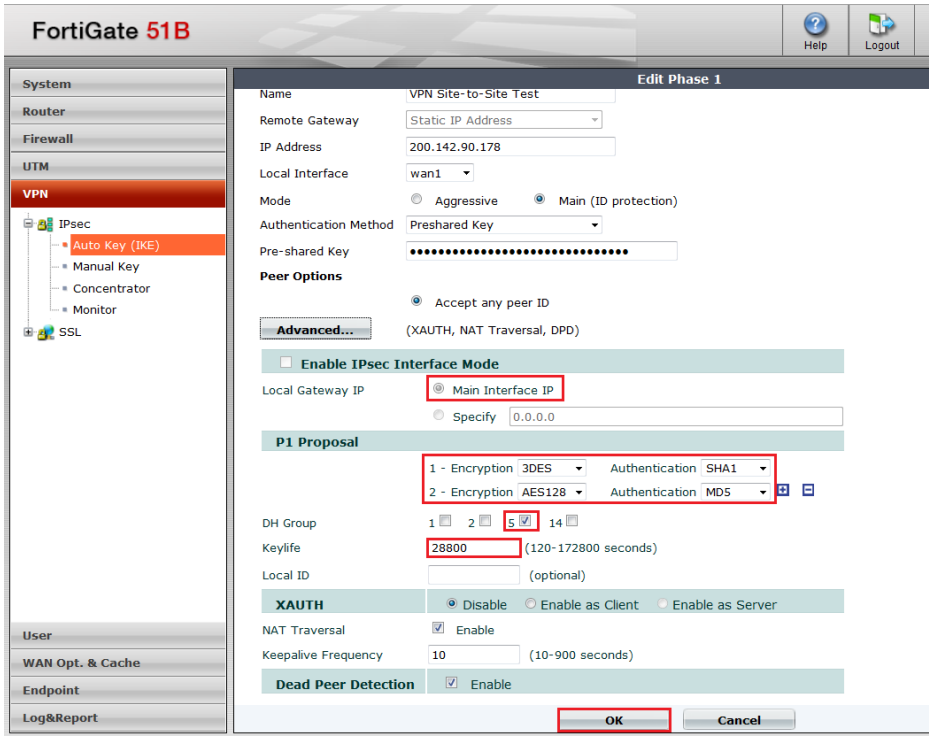
As telas apresentadas a seguir apresentam a configuração de uma VPN Site-to-Site parao cenário abaixo:

- Site A: Gateway = 200.202.114.250 - Rede=10.123.123.0/24
- Site B: Gateway = 200.142.90.178 – Rede = 10.55.1.0/24

11.1 Fase 1

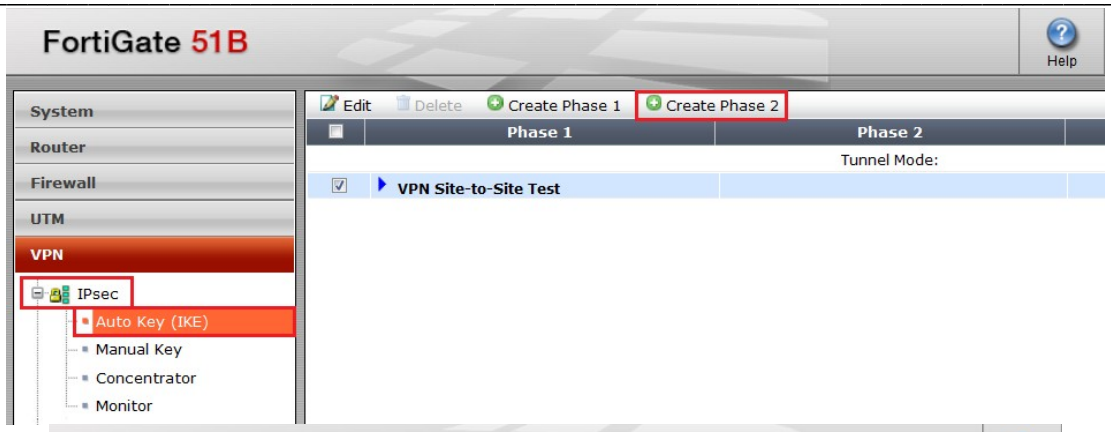


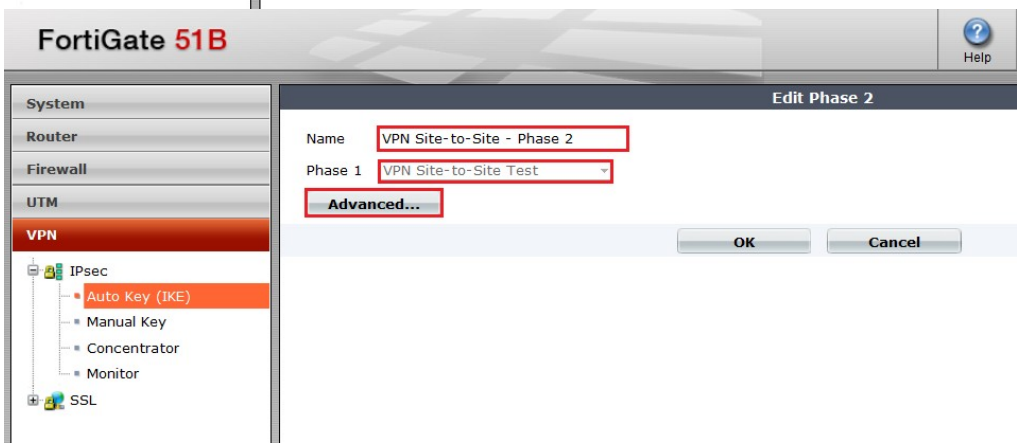


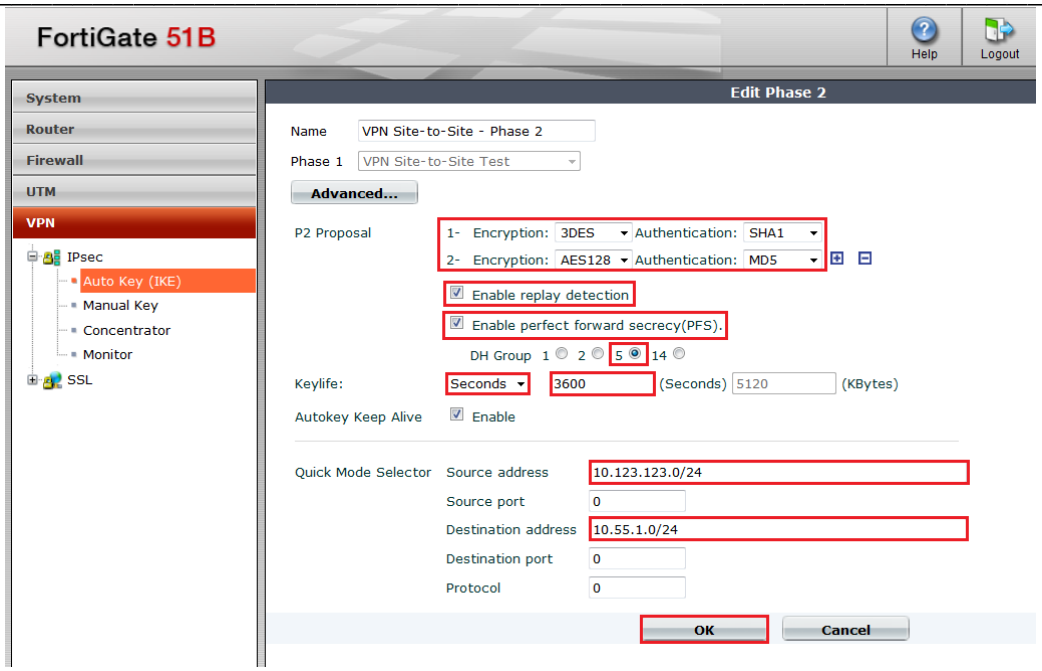


11.2 Fase 2

***Observação**: após a configuração da Fase 2 a VPN não se tornará ativa. A VPN estará ativa apenas após a criação das regras de firewall referente ao tráfego a ser enviado pelo túnel.


FortiGate 51B
Help
System
Router
Firewall
UTM
VPN
IPsec
Auto Key (IKE)
Manual Key
Concentrator
Monitor
Edit
Delete
Create Phase 1
Create Phase 2
Phase 1
Phase 2
Tunnel Mode:
VPN Site-to-Site Test

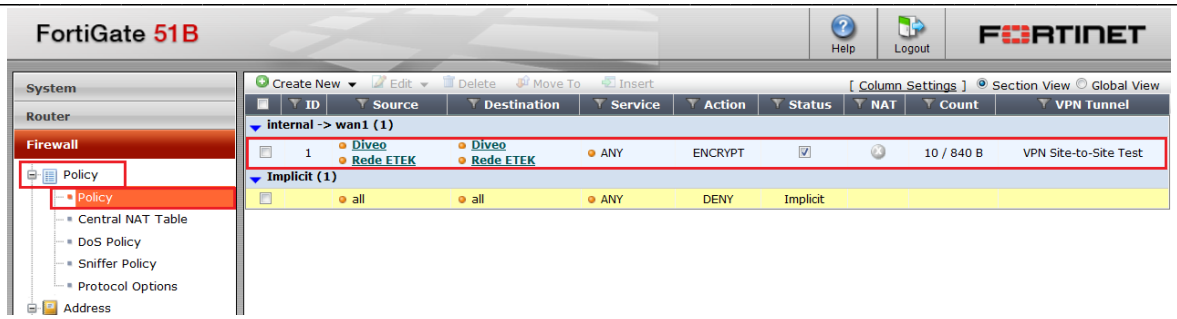

FortiGate 51B
Help
System
Router
Firewall
UTM
VPN
IPsec
Auto Key (IKE)
Manual Key
Concentrator
Monitor
SSL
Edit Phase 2
Name
VPN Site-to-Site - Phase 2
Phase 1
VPN Site-to-Site Test
Advanced...
OK
Cancel

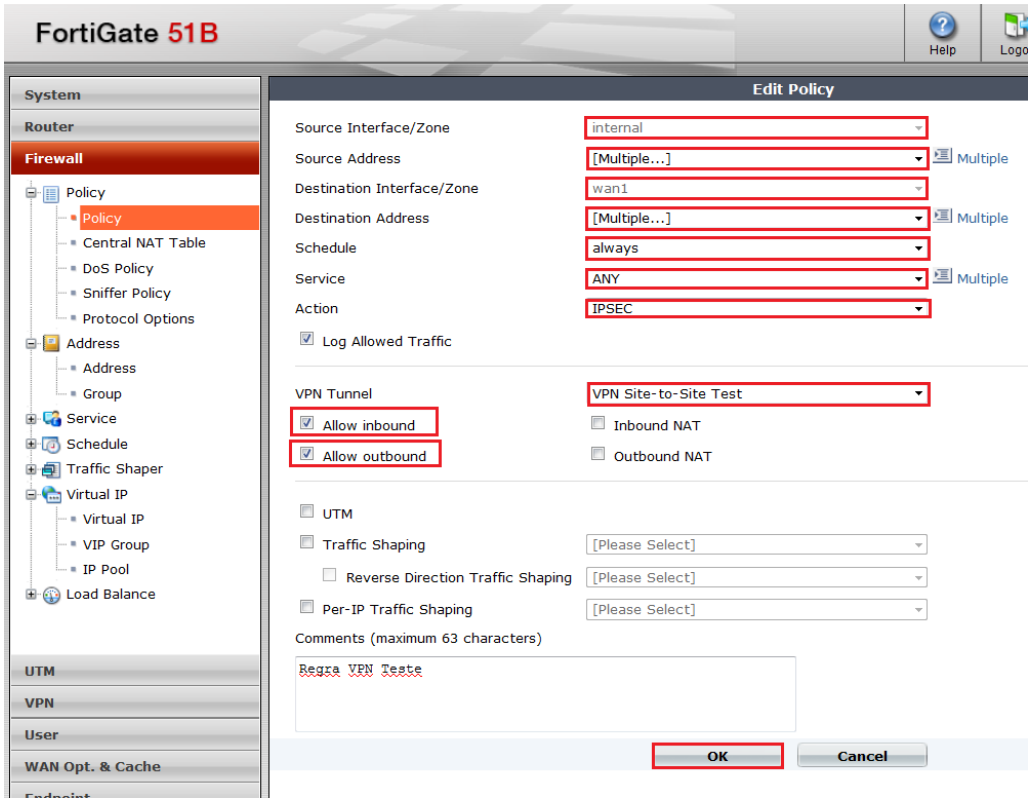


***Observação**: Em situações em que o Source address ou o Destination address devem ser preenchidos com mais de uma rede deve-se criar uma configuração de Fase 2 *para cada rede*.

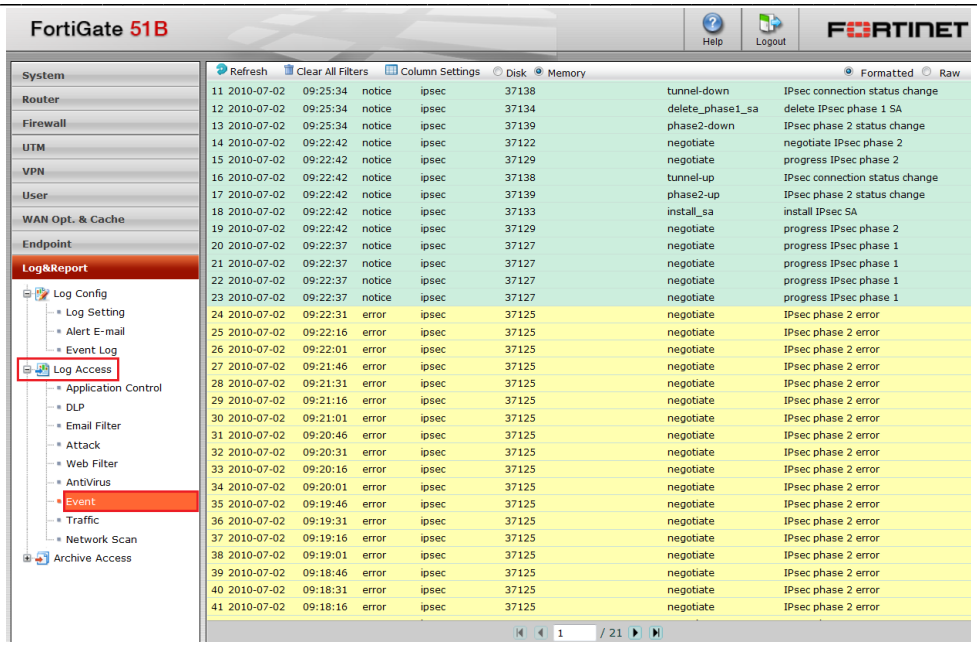
11.3 Regras

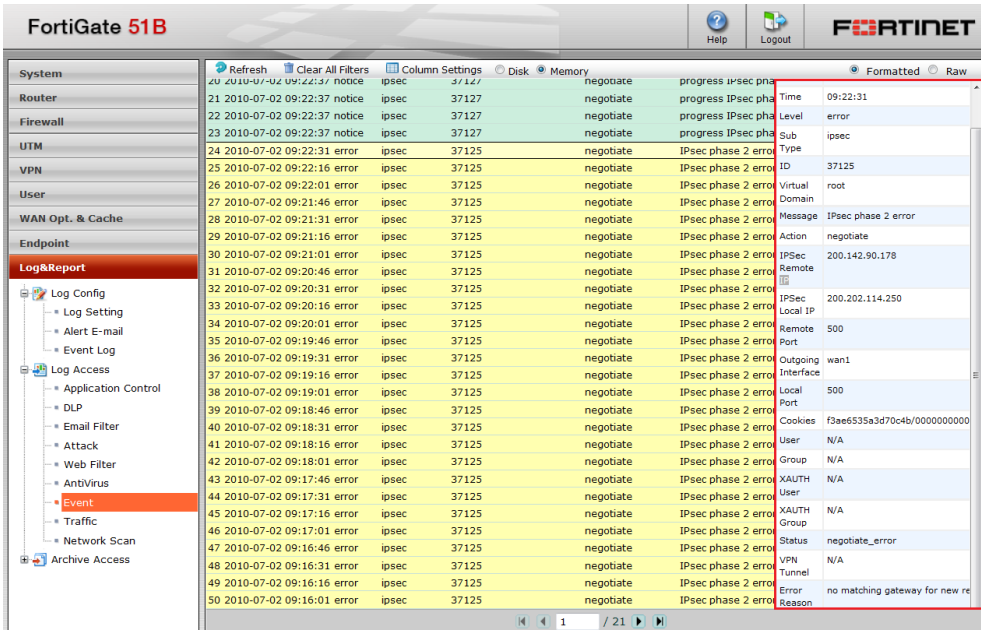
- Rede Site A = Diveo =10.123.123.0/24
- Rede Site B = Etek = 10.55.1.0/24

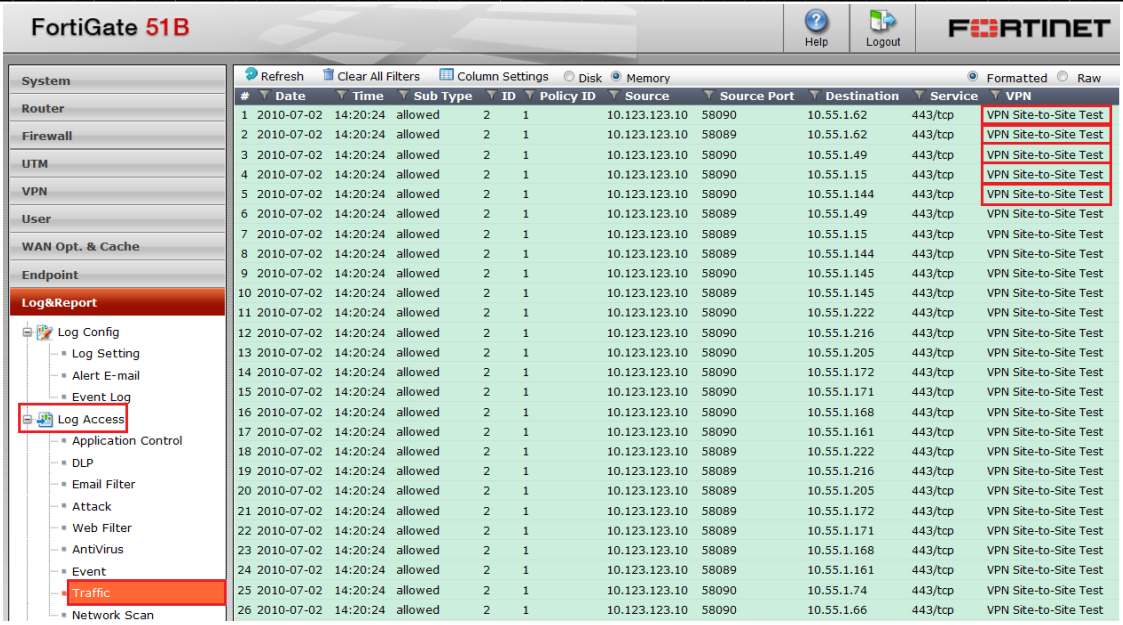




11.4 Monitoração

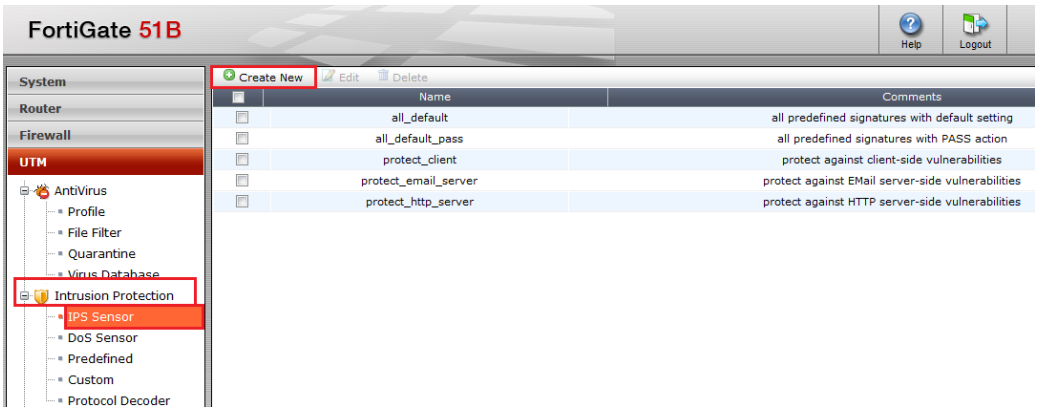

FortiGate 51B
Help
Logout
FORTINET
System
Router
Firewall
UTM
VPN
User
WAN Opt. & Cache
Endpoint
Log&Report
Log Config
Log Setting
Alert E-mail
Event Log
Log Access
Application Control
DLP
Email Filter
Attack
Web Filter
AntiVirus
Event
Traffic
Network Scan
Archive Access
Refresh
Clear All Filters
Column Settings
Disk
Memory
Formatted
Raw
11 2010-07-02 09:25:34 notice ipsec 37138 tunnel-down IPsec connection status change
12 2010-07-02 09:25:34 notice ipsec 37134 delete_phase1_sa delete IPsec phase 1 SA
13 2010-07-02 09:25:34 notice ipsec 37139 phase2-down IPsec phase 2 status change
14 2010-07-02 09:22:42 notice ipsec 37122 negotiate negotiate IPsec phase 2
15 2010-07-02 09:22:42 notice ipsec 37129 negotiate progress IPsec phase 2
16 2010-07-02 09:22:42 notice ipsec 37138 tunnel-up IPsec connection status change
17 2010-07-02 09:22:42 notice ipsec 37139 phase2-up IPsec phase 2 status change
18 2010-07-02 09:22:42 notice ipsec 37133 install_sa install IPsec SA
19 2010-07-02 09:22:42 notice ipsec 37129 negotiate progress IPsec phase 2
20 2010-07-02 09:22:37 notice ipsec 37127 negotiate progress IPsec phase 1
21 2010-07-02 09:22:37 notice ipsec 37127 negotiate progress IPsec phase 1
22 2010-07-02 09:22:37 notice ipsec 37127 negotiate progress IPsec phase 1
23 2010-07-02 09:22:37 notice ipsec 37127 negotiate progress IPsec phase 1
24 2010-07-02 09:22:31 error ipsec 37125 negotiate IPsec phase 2 error
25 2010-07-02 09:22:16 error ipsec 37125 negotiate IPsec phase 2 error
26 2010-07-02 09:22:01 error ipsec 37125 negotiate IPsec phase 2 error
27 2010-07-02 09:21:46 error ipsec 37125 negotiate IPsec phase 2 error
28 2010-07-02 09:21:31 error ipsec 37125 negotiate IPsec phase 2 error
29 2010-07-02 09:21:16 error ipsec 37125 negotiate IPsec phase 2 error
30 2010-07-02 09:21:01 error ipsec 37125 negotiate IPsec phase 2 error
31 2010-07-02 09:20:46 error ipsec 37125 negotiate IPsec phase 2 error
32 2010-07-02 09:20:31 error ipsec 37125 negotiate IPsec phase 2 error
33 2010-07-02 09:20:16 error ipsec 37125 negotiate IPsec phase 2 error
34 2010-07-02 09:20:01 error ipsec 37125 negotiate IPsec phase 2 error
35 2010-07-02 09:19:46 error ipsec 37125 negotiate IPsec phase 2 error
36 2010-07-02 09:19:31 error ipsec 37125 negotiate IPsec phase 2 error
37 2010-07-02 09:19:16 error ipsec 37125 negotiate IPsec phase 2 error
38 2010-07-02 09:19:01 error ipsec 37125 negotiate IPsec phase 2 error
39 2010-07-02 09:18:46 error ipsec 37125 negotiate IPsec phase 2 error
40 2010-07-02 09:18:31 error ipsec 37125 negotiate IPsec phase 2 error
41 2010-07-02 09:18:16 error ipsec 37125 negotiate IPsec phase 2 error
1 / 21

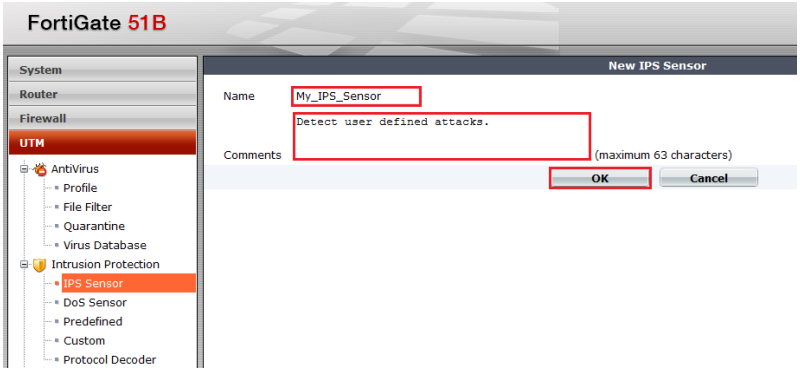

FortiGate 51B
Help
Logout
FORTINET
System
Router
Firewall
UTM
VPN
User
WAN Opt. & Cache
Endpoint
Log&Report
Log Config
Log Setting
Alert E-mail
Event Log
Log Access
Application Control
DLP
Email Filter
Attack
Web Filter
AntiVirus
Event
Traffic
Network Scan
Archive Access
Refresh
Clear All Filters
Column Settings
Disk
Memory
Formatted
Raw
Time 09:22:31
Level error
Sub Type ipsec
ID 37125
Virtual Domain root
Message IPsec phase 2 error
Action negotiate
IPSec Remote 200.142.90.178
IPSec Local IP 200.202.114.250
Remote Port 500
Outgoing Interface wan1
Local Port 500
Cookies f3ae6535a3d70c4b/0000000000
User N/A
Group N/A
XAUTH User N/A
XAUTH Group N/A
Status negotiate_error
VPN Tunnel N/A
Error Reason no matching gateway for new re
1 / 21



12 IPS

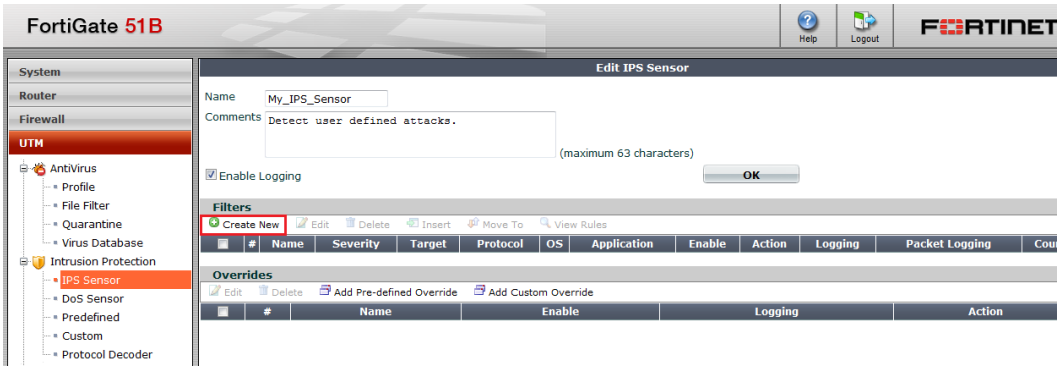
12.1 IPS Sensor

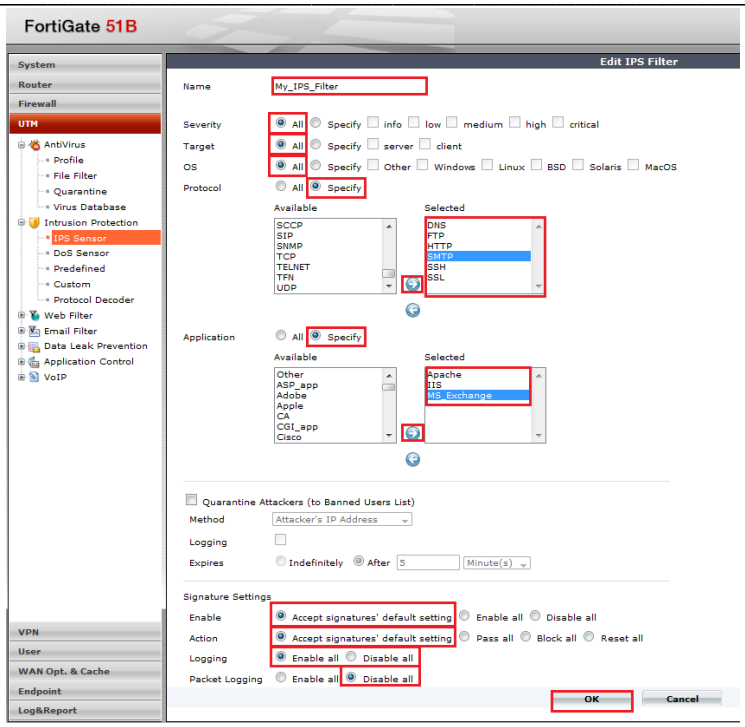




12.2 Filtro

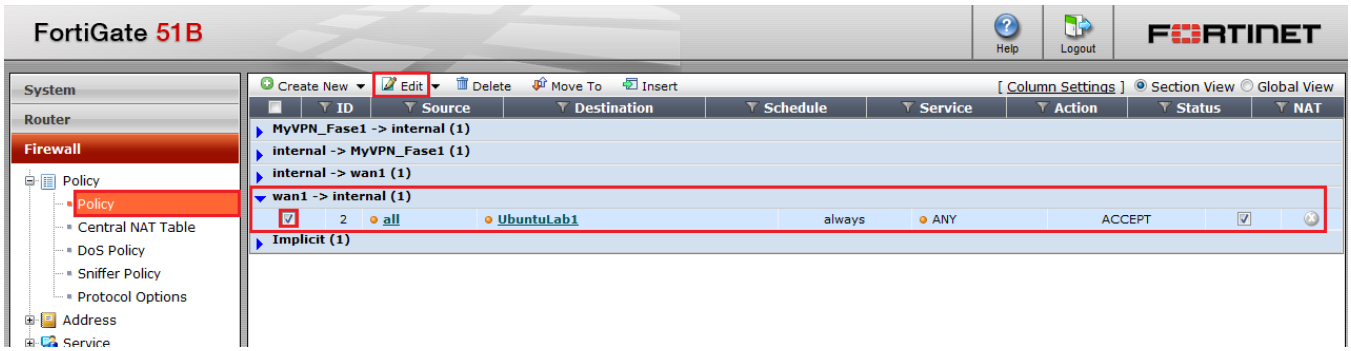
Através do filtro são definidos os grupos de protocolos e aplicações que serão analisados.

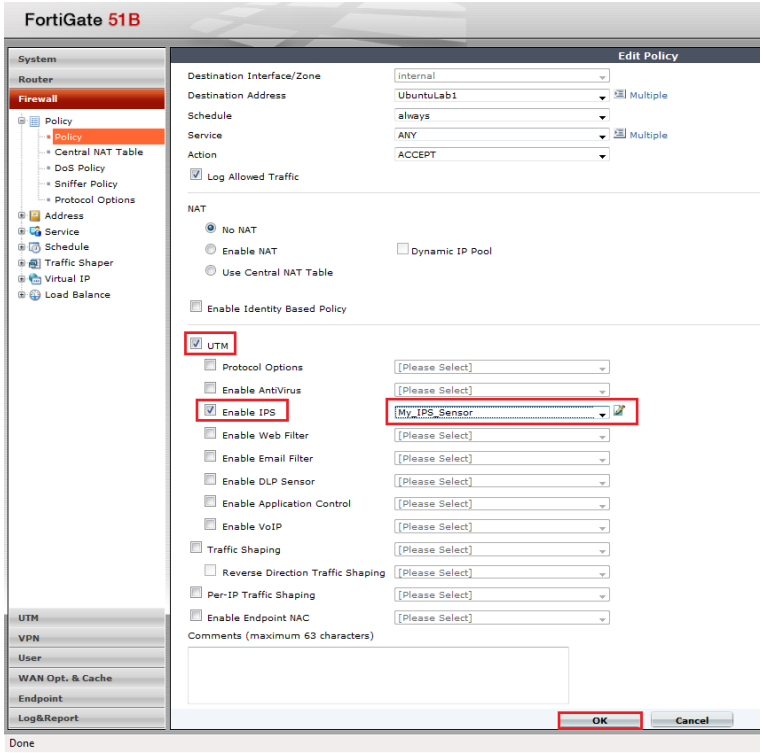




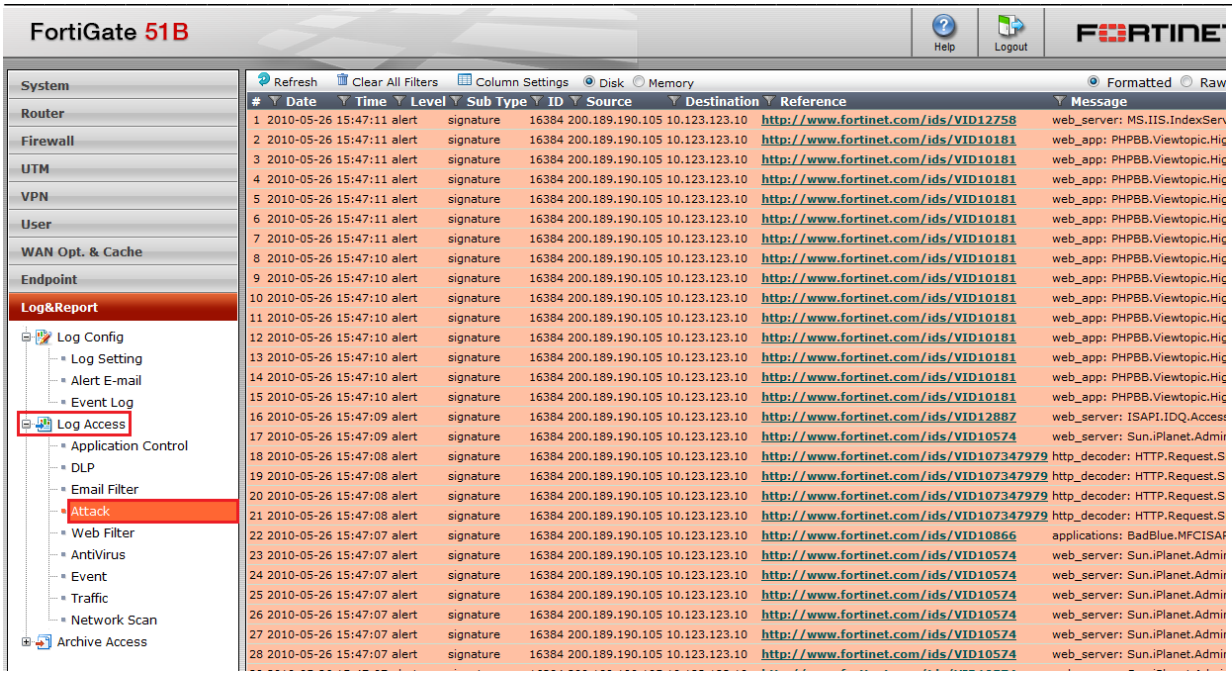
12.3 Regra de Firewall

Selecionar a regra de firewall que terá seu tráfego analisado:

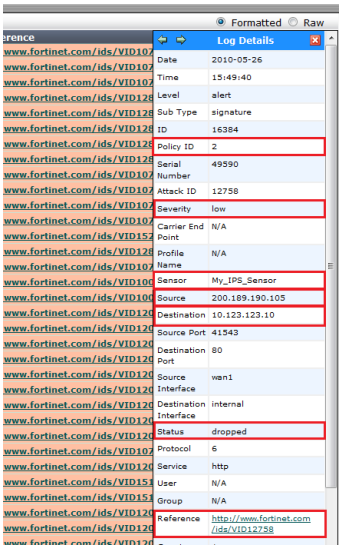




12.4 Log de Ataques

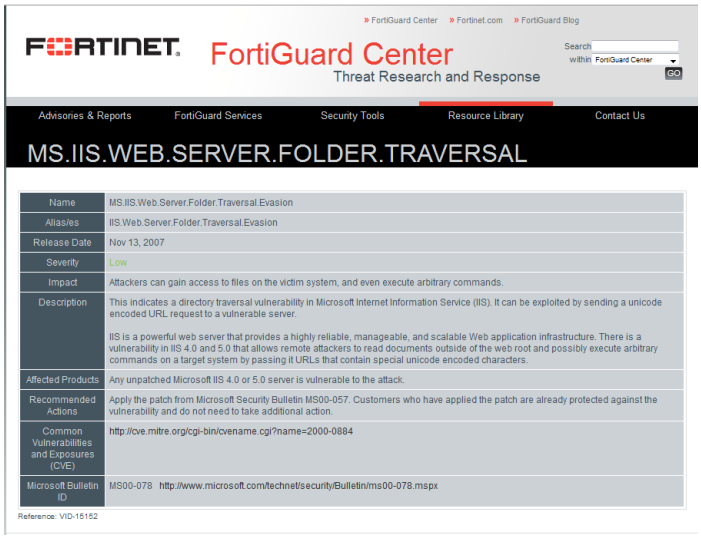


Selecionando uma linha de ataque pode-se obter mais detalhes do ataque: policy ID (número da regra), sensor utilizado na detecção, status (dropped/detected), criticidade (severity), etc...

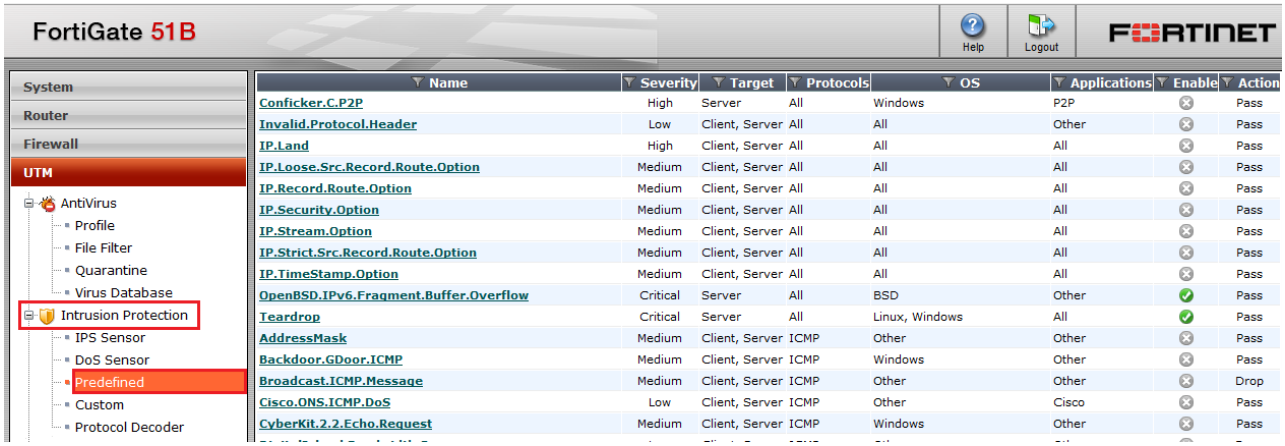


Mais detalhes sobre cada ataque podem ser obtidos através do link apresentado no campo Reference:

78	2010-05-26 15:50:22	alert	signature	16384	200.189.190.105	10.123.123.10	http://www.fortinet.com/ids/VID12015	web_server: MS.IIS.Web.Server
79	2010-05-26 15:50:22	alert	signature	16384	200.189.190.105	10.123.123.10	http://www.fortinet.com/ids/VID15152	web_server: MS.IIS.Web.Server
80	2010-05-26 15:50:22	alert	signature	16384	200.189.190.105	10.123.123.10	http://www.fortinet.com/ids/VID15152	web_server: MS.IIS.Web.Server
81	2010-05-26 15:50:22	alert	signature	16384	200.189.190.105	10.123.123.10	http://www.fortinet.com/ids/VID12015	web_server: MS.IIS.Web.Server



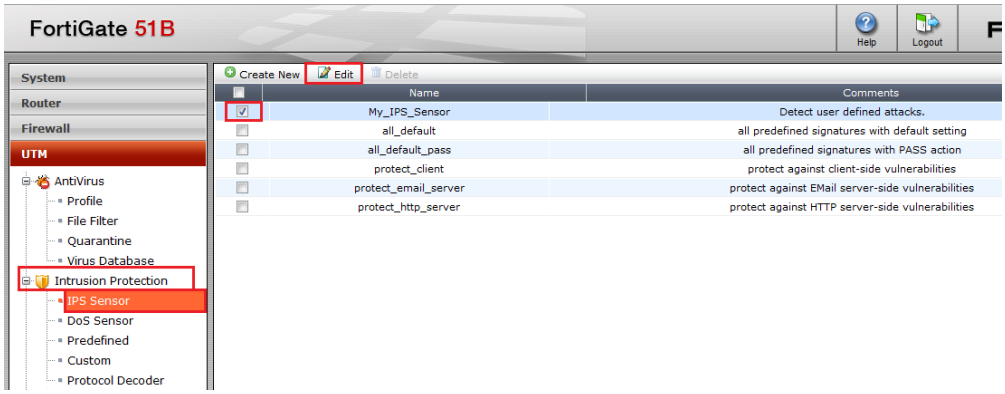
12.5 Assinaturas de Ataques Pré-definidas



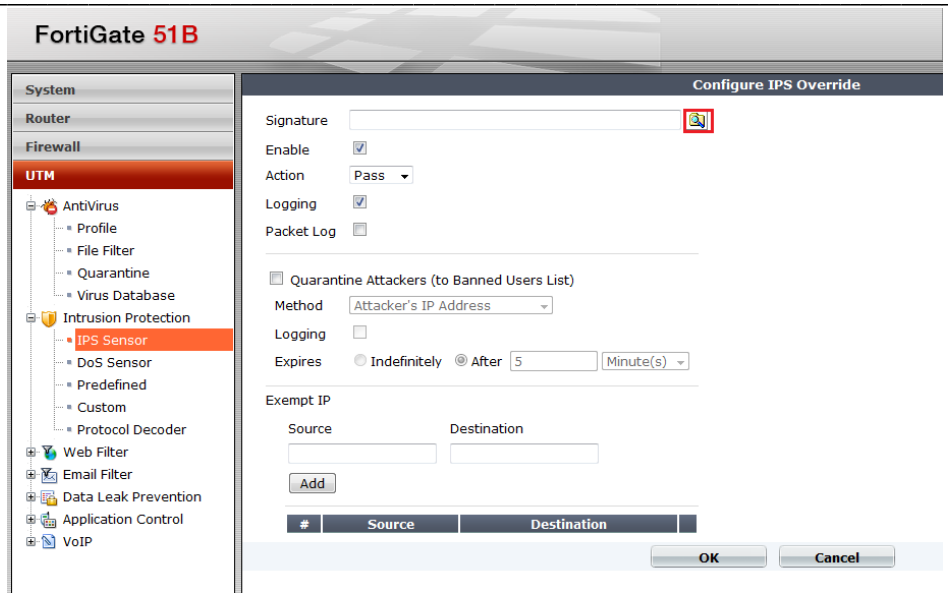
12.6 Alterar o Comportamento de uma Assinatura e White-list

O comportamento padrão das assinaturas pode ser alterado através da configuração de "overrides" do IPS Sensor desejado. Quando uma assinatura pré-

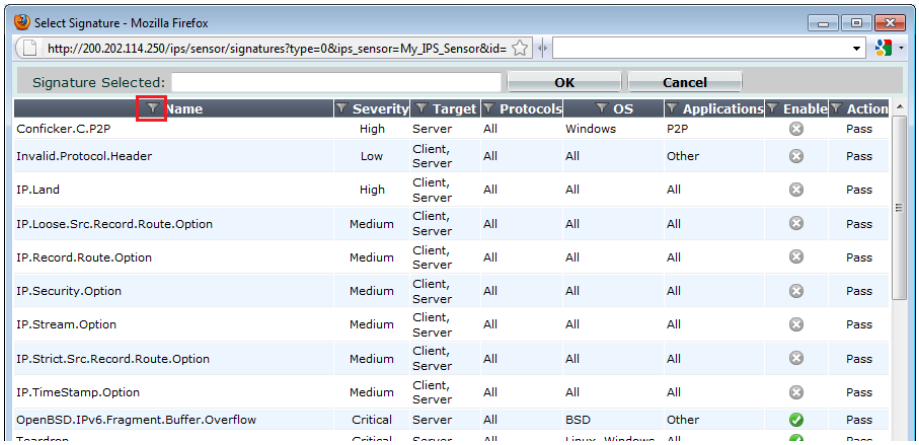
definida (já existente) é especificada em um override o seu comportamento padrão (default) será ignorado.

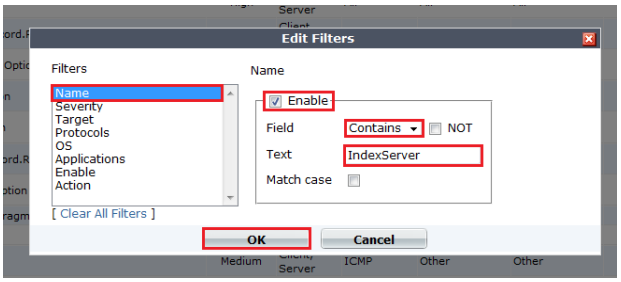


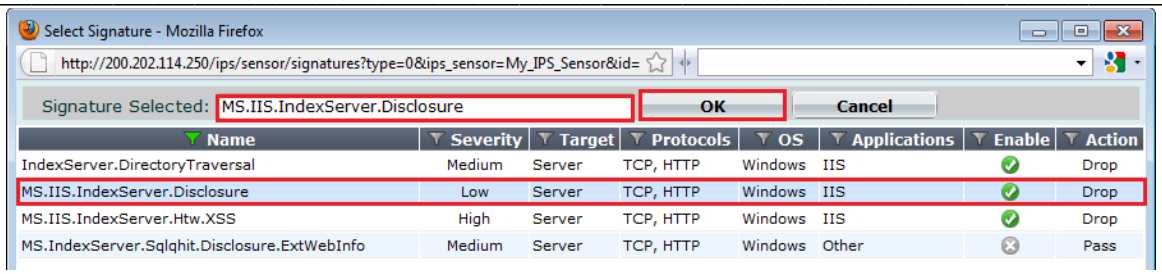
Para fazer o override de uma assinatura padrão deve-se selecionar a opção "Add Pre-definided Override".



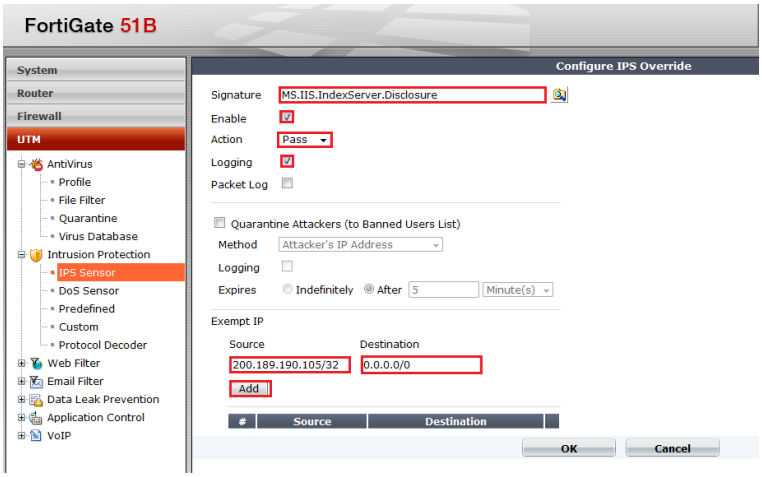
Usar o filtro de nome para encontrar a assinatura desejada:

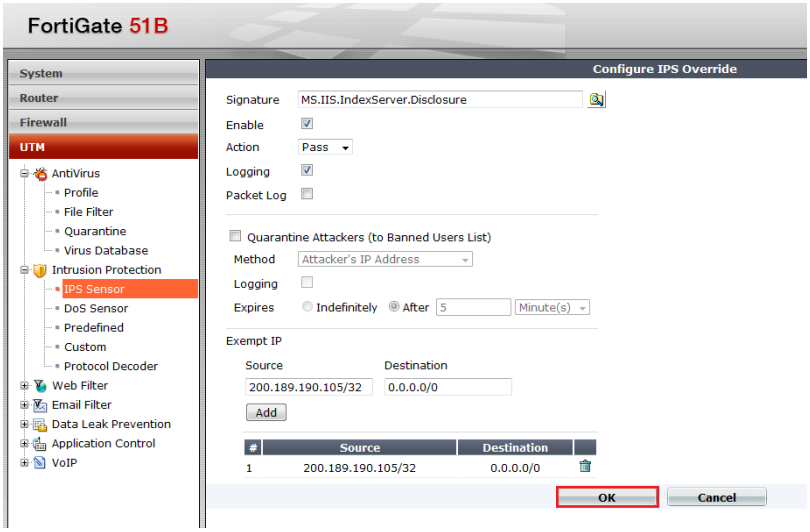


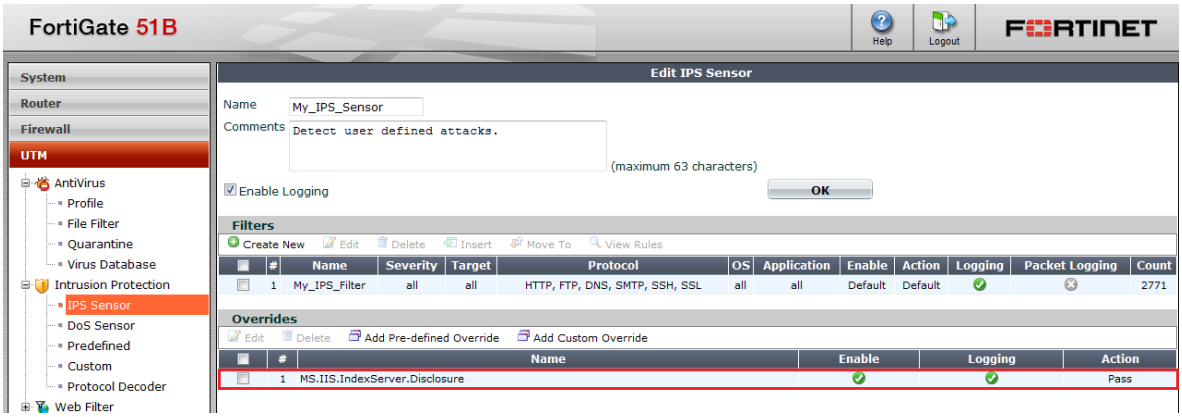




Pode-se então definir um novo comportamento para a assinatura desejada. A configuração abaixo cria um white-list para o endereço 200.189.190.105, especificamente para esta assinatura:





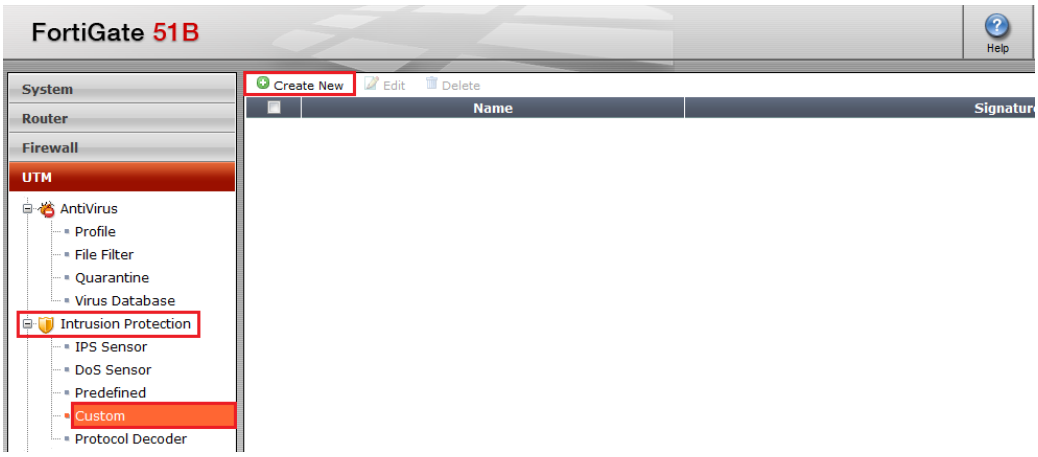


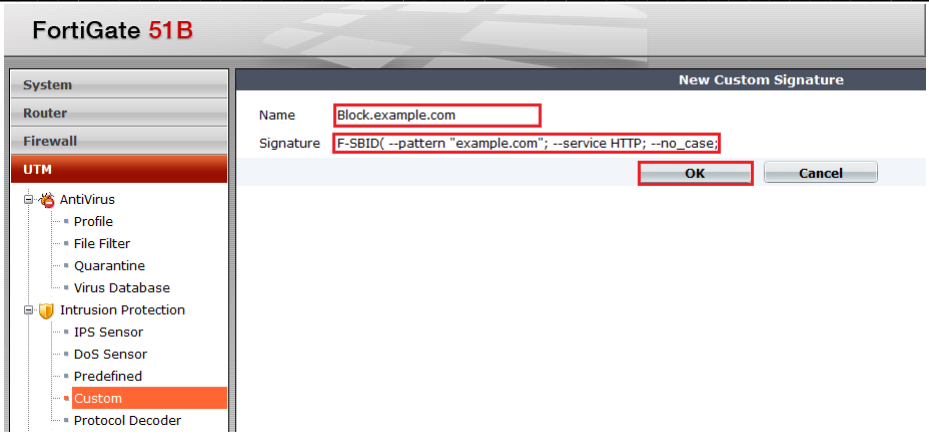
12.7 Criar uma Assinatura Customizada

O processo de criação de assinaturas customizadas é apresentado no documento "Fortigate UTM User Guide".

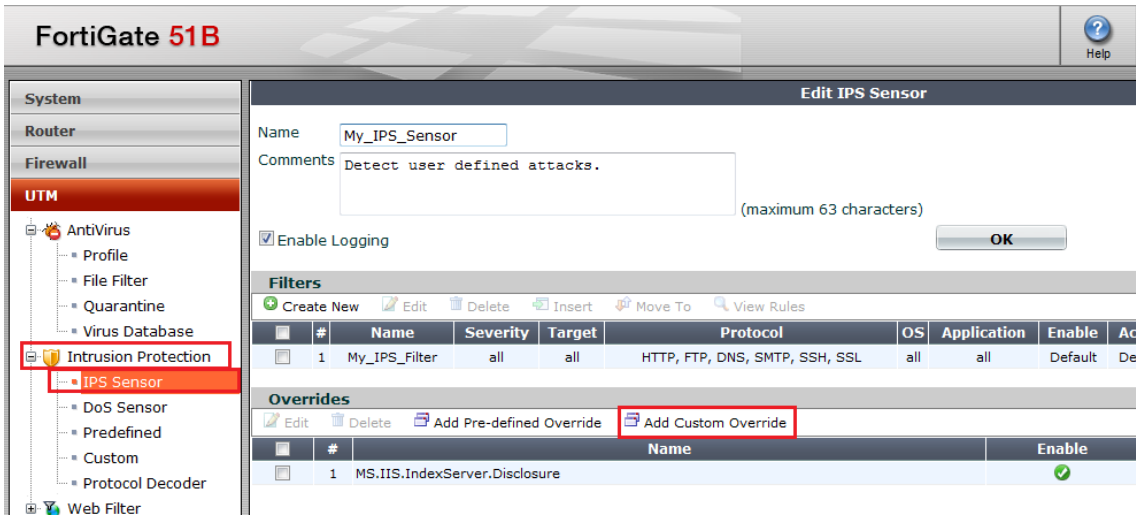
Para criar uma assinatura para bloquear o acesso ao site "example.com" deve-se preencher a tela new custom signatures com os valores:

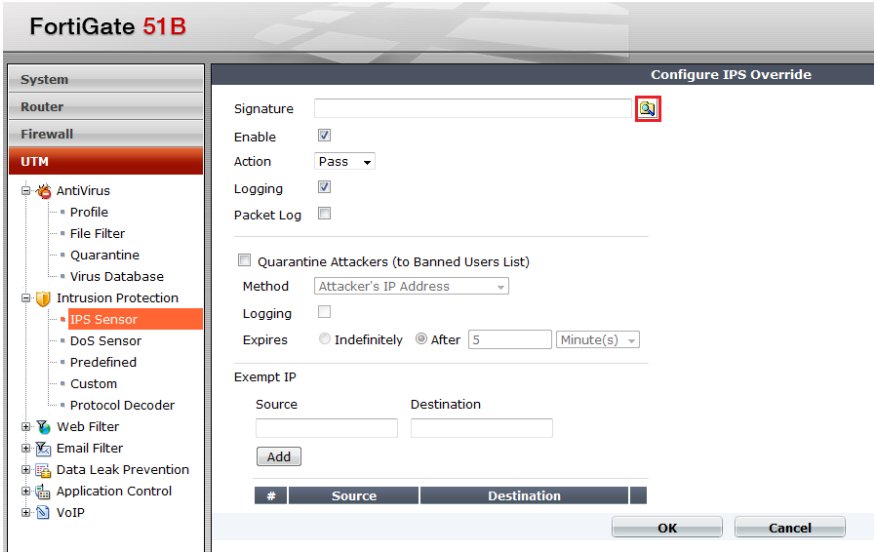
Name: Block.example.com
Signature: F-SBID(--pattern "example.com"; --service HTTP; --no_case; --flow from_client; --context host;)

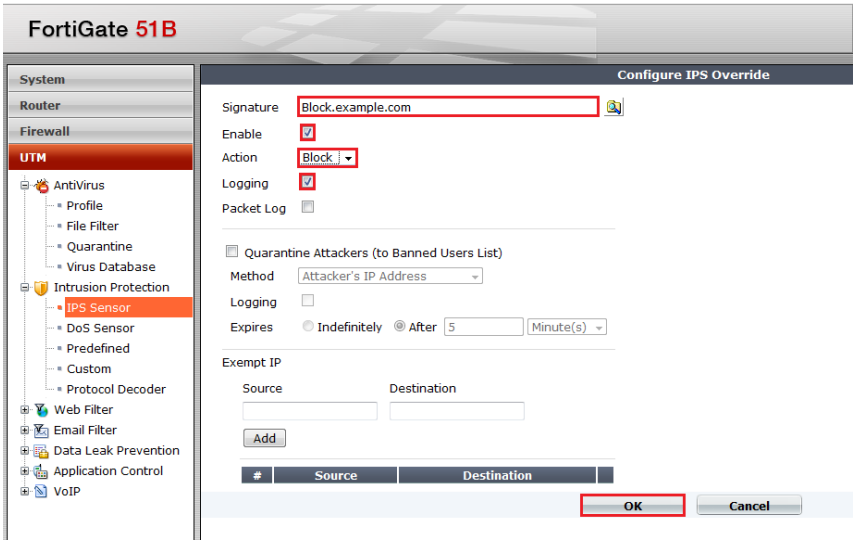




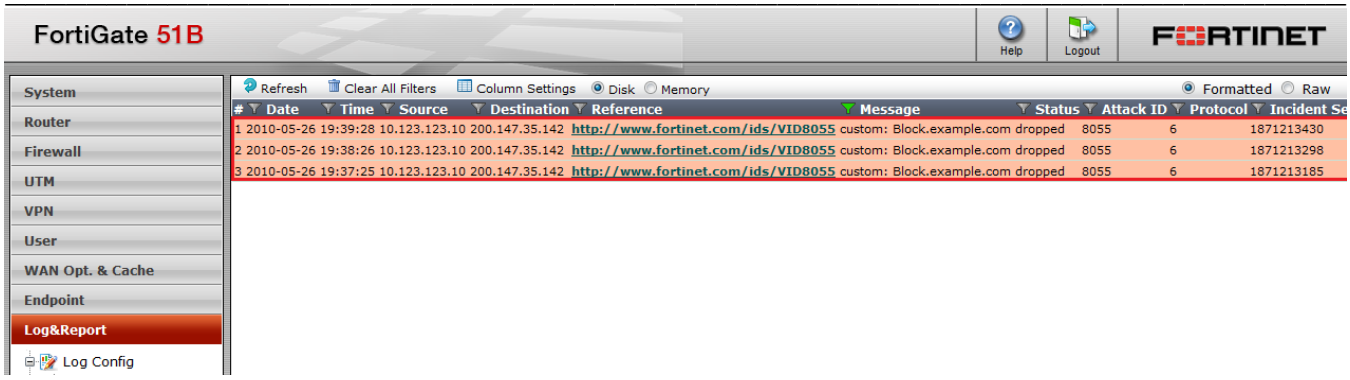
Deve-se adicionar a nova assinatura ao IPS Sensor desejado através de um Custom Override:







O log deverá mostrar as ocorrências de um evento detectado pela nova assinatura:



12.8 Configurar Horário de Atualização de Assinaturas

Para configurar as atualizações das assinaturas do IPS deve-se utilizar os comandos abaixo:

```
# config system autoupdate schedule
(schedule) # set frequency daily
(schedule) # set time 01:00
(schedule) # end
```

Para atualizações com frequencia menor que um dia pode-se usar o "commando set frequency every" no lugar do "set frequency daily" (como mostrado acima). Neste caso o commando "set time" definirá" o interval entre as atualizações e não mais a hora da atualização. Exemplo:

```
# config system autoupdate schedule
(schedule) # set frequency every
(schedule) # set time 01:00
(schedule) # end
```

Pode-se verificar o schedule de atualização através do commando "get system autoupdate schedule". Exemplo:

```
# get system autoupdate schedule
frequency           : daily
status              : enable
time                : 01:00
```

Para atualizar manualmente as assinaturas pode-se usar o comando "execute update-ips":

```
# execute update-ips
```

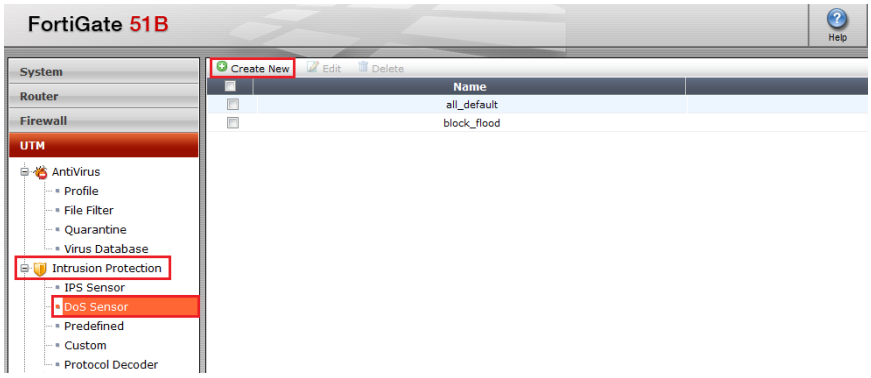
Este comando não emite mensagem alguma, no entanto pode-se verificar o resultado da operação através do comando "get system auto-update versions" e observar as seções "Attack Definitions" e "IPS Attack Engines":

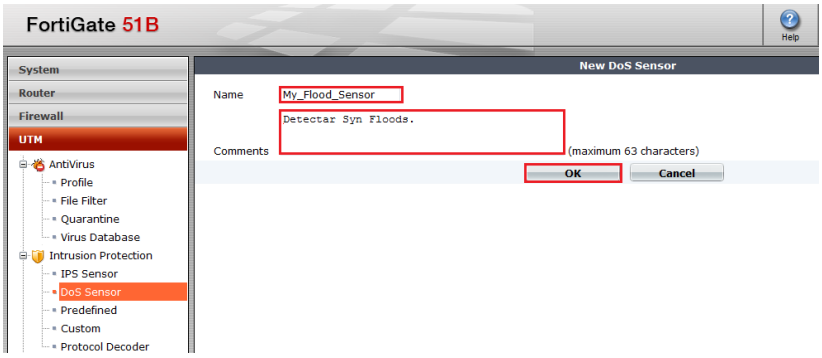
```
# get system auto-update versions
...
Attack Definitions
---------
Version: 2.00988
Contract Expiry Date: Sun Apr 29 00:00:00 2012
Last Updated using manual update on Wed Apr 27 15:20:35 2011
Last Update Attempt: Wed Apr 27 16:28:46 2011
Result: No Updates

IPS Attack Engine
---------
Version: 1.00171
Contract Expiry Date: Sun Apr 29 00:00:00 2012
Last Updated using manual update on Tue Nov  2 16:06:00 2010
Last Update Attempt: Wed Apr 27 16:28:46 2011
Result: No Updates
...
```

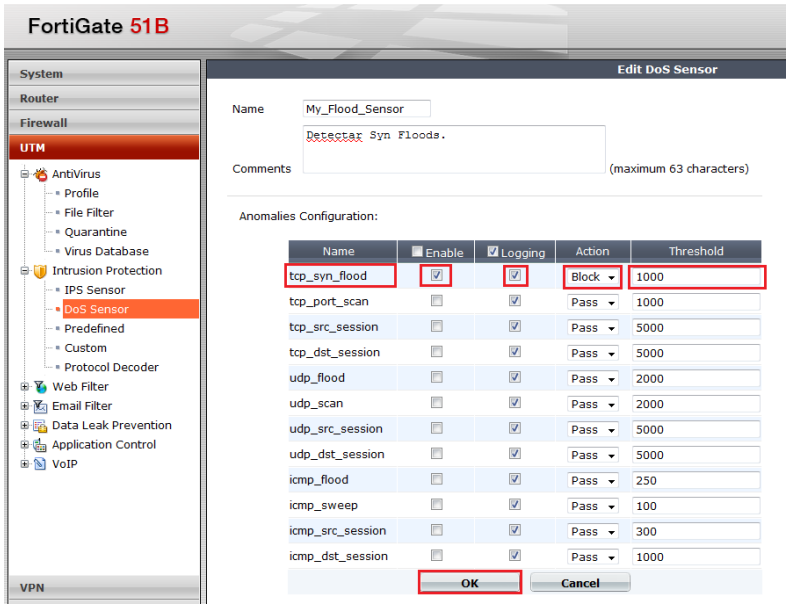
13 DoS Sensor

Além dos ataques baseados em assianturas o Fortigate pode detetar ataques baseados em comportamento de rede (floods). Para isto é usado o Dos Sensor.

13.1 Syn Flood

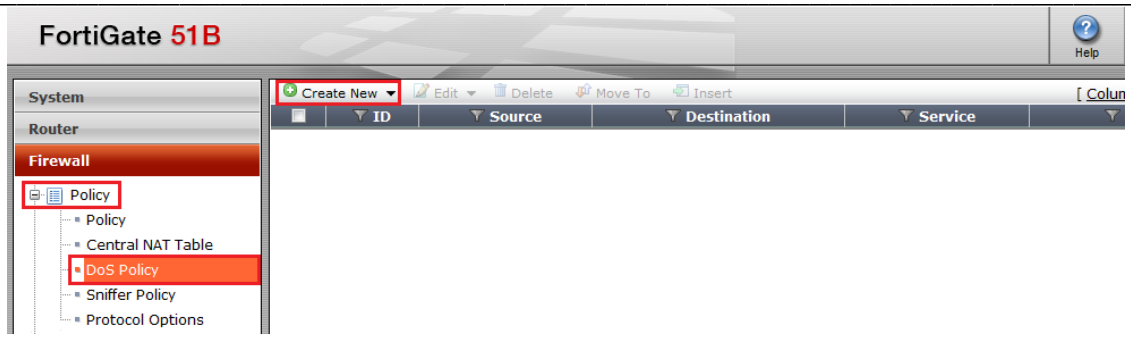


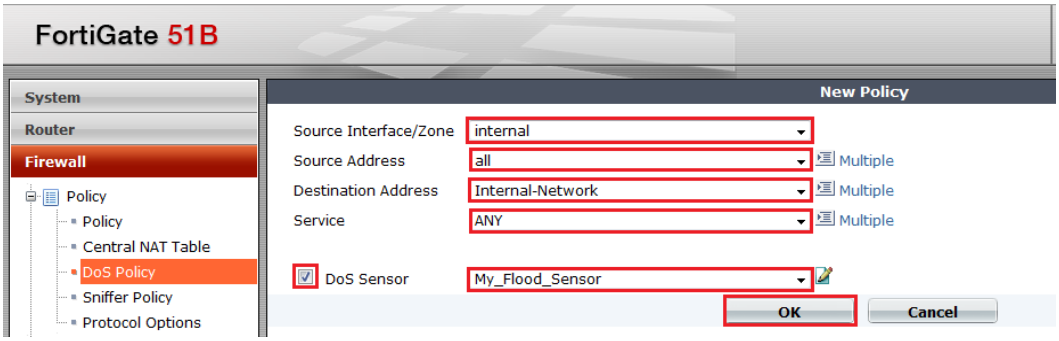


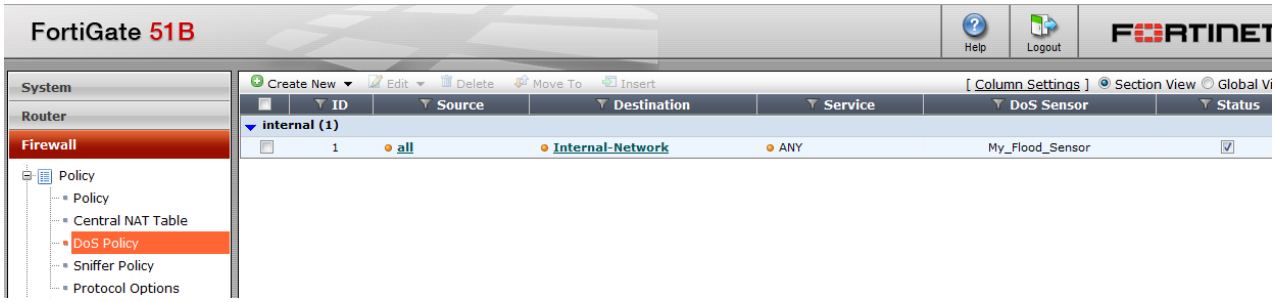


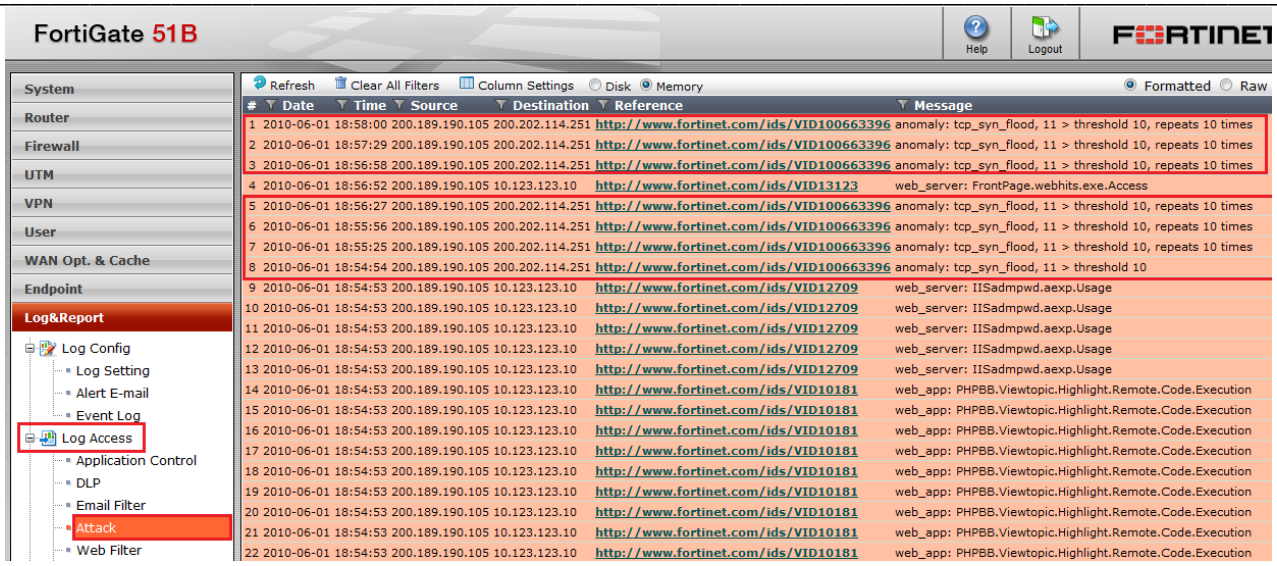
Em equipamentos de maior porte pode-se usar o mecanismo de syn Proxy que é mais eficiente que o mecanismo de block:

"With a Fortinet security processing module installed, FortiGate units that support these modules offer a third action for the `tcp_syn_flood` threshold. In addition to *Block* and *Pass*, you can choose to *Proxy* connect attempts when their volume exceeds the threshold value. When the `tcp_syn_flood` threshold action is set to *Proxy*, incomplete TCP connections are allowed as normal as long as the configured threshold is not exceeded. If the threshold is exceeded, the FortiGate unit will intercept incoming SYN packets with a hardware accelerated SYN proxy to determine whether the connection attempts are legitimate or a SYN flood attack. Legitimate connections are allowed while an attack is blocked."


FortiGate 51B
Help
System
Router
Firewall
Policy
Policy
Central NAT Table
DoS Policy
Sniffer Policy
Protocol Options
Create New
Edit
Delete
Move To
Insert
ID
Source
Destination
Service


FortiGate 51B
System
Router
Firewall
Policy
Policy
Central NAT Table
DoS Policy
Sniffer Policy
Protocol Options
New Policy
Source Interface/Zone
internal
Source Address
all
Multiple
Destination Address
Internal-Network
Multiple
Service
ANY
Multiple
DoS Sensor
My_Flood_Sensor
OK
Cancel


FortiGate 51B
Help
Logout
FORTINET
System
Router
Firewall
Policy
Policy
Central NAT Table
DoS Policy
Sniffer Policy
Protocol Options
Create New
Edit
Delete
Move To
Insert
[Column Settings]
Section View
Global Vi
ID
Source
Destination
Service
DoS Sensor
Status
internal (1)
1
all
Internal-Network
ANY
My_Flood_Sensor

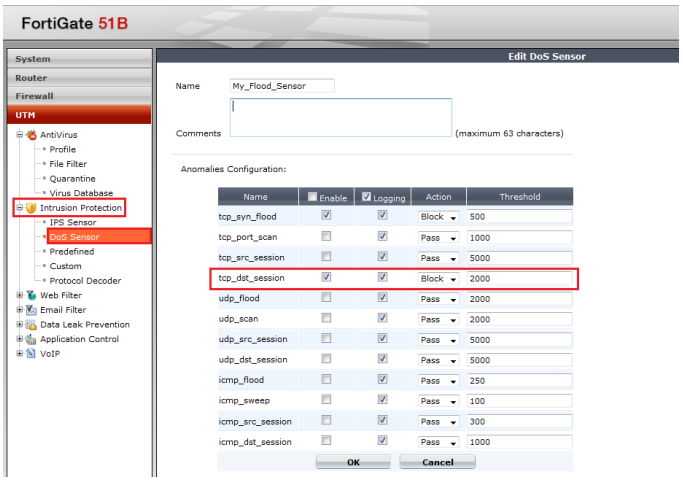


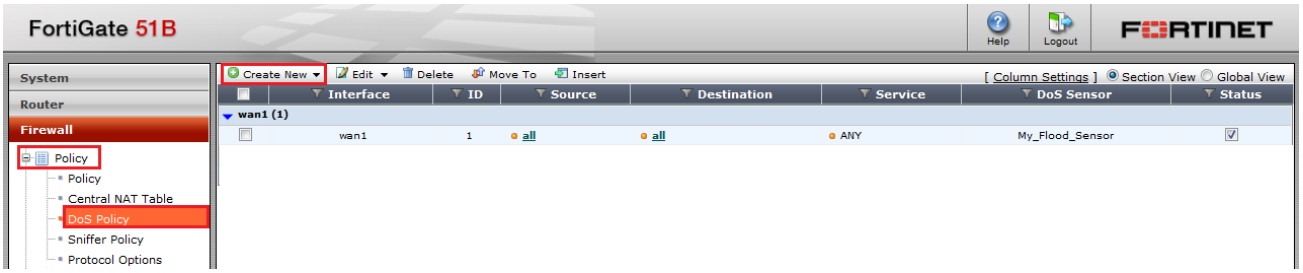

```
root@UbuntuLucid1:/var/log# tail -f fortigate.log | grep Flood
Jun  1 18:52:52 10.123.123.1 date=2010-06-01 time=18:53:14 devname=Fortigate51B
device_id=FG50BH3G09600388 log_id=0104032162 type=event subtype=admin pri=notice
vd=root user="admin" ui=GUI(200.162.31.4) msg="User admin changed sensor
My_Flood_Sensor"

Jun  1 18:54:32 10.123.123.1 date=2010-06-01 time=18:54:54 devname=Fortigate51B
device_id=FG50BH3G09600388 log_id=0420018432 type=ips subtype=anomaly pri=alert
severity=critical carrier_ep="N/A" vd="N/A" vd="N/A" profile="N/A"
src=200.189.190.105 dst=200.202.114.251 src_int="wan1" dst_int="N/A" policyid=N/A
identidx=N/A serial=0 status=clear_session proto=6 service=http vd="root" count=1
src_port=50279 dst_port=80 attack_id=100663396 sensor="My_Flood_Sensor"
ref="http://www.fortinet.com/ids/VID100663396" user="N/A" group="N/A" msg="anomaly:
tcp_syn_flood, 11 > threshold 10"

Jun  1 18:55:03 10.123.123.1 date=2010-06-01 time=18:55:25 devname=Fortigate51B
device_id=FG50BH3G09600388 log_id=0420018432 type=ips subtype=anomaly pri=alert
severity=critical carrier_ep="N/A" vd="N/A" vd="N/A" profile="N/A"
src=200.189.190.105 dst=200.202.114.251 src_int="wan1" dst_int="N/A" policyid=N/A
identidx=N/A serial=0 status=clear_session proto=6 service=http vd="root" count=10
src_port=59627 dst_port=80 attack_id=100663396 sensor="My_Flood_Sensor"
ref="http://www.fortinet.com/ids/VID100663396" user="N/A" group="N/A" msg="anomaly:
tcp_syn_flood, 11 > threshold 10, repeats 10 times"
```

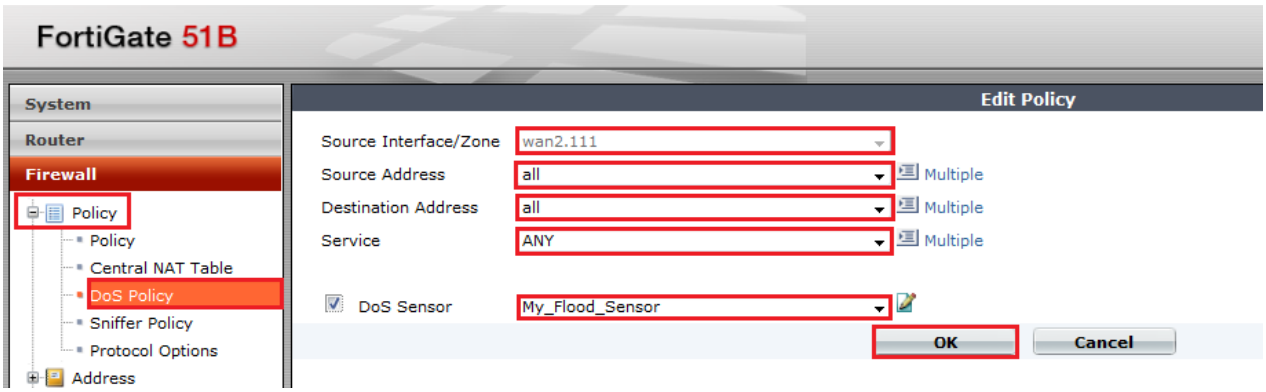
13.2 Limite de Sessões Por Destino

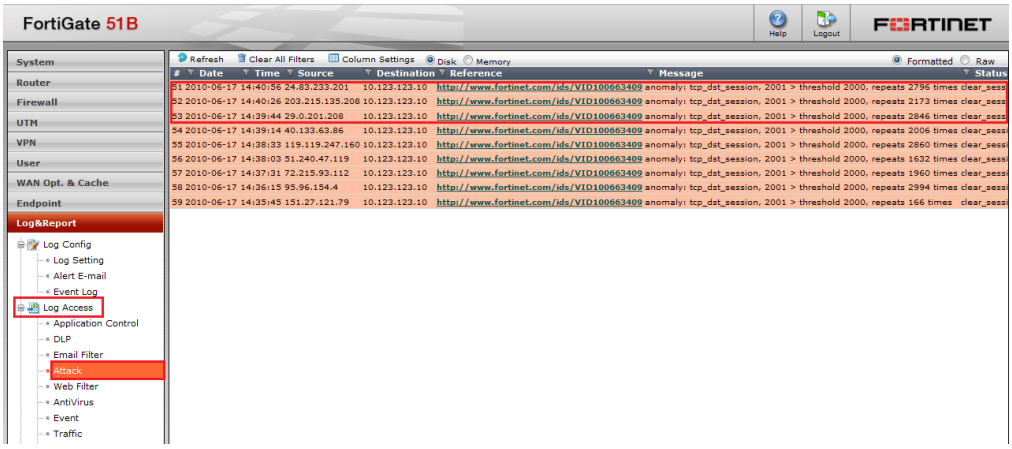
O mecanismo de limite de sessões por endereço de destino deve ser usado quando os endereços de origem são falsos e aleatórios (spoofed source address).

Através deste mecanismo, quando o número de sessões para um endereço destino for atingido, as demais conexões para o mesmo endereço serão descartadas. Isto fará com que o endereço destino deixe de ser acessado mesmo por usuários válidos. Este mecanismo, no entanto, evita que todos os recursos de memória e processamento sejam exauridos, assim impedindo que todo o equipamento e os demais recursos por ele protegido sejam afetados.

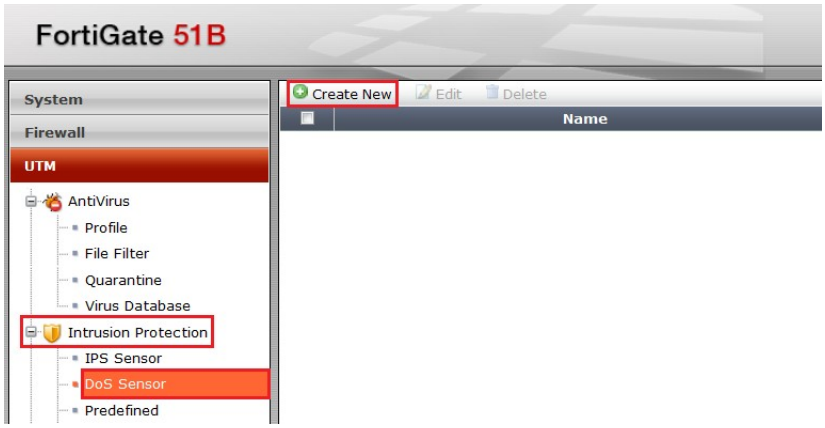


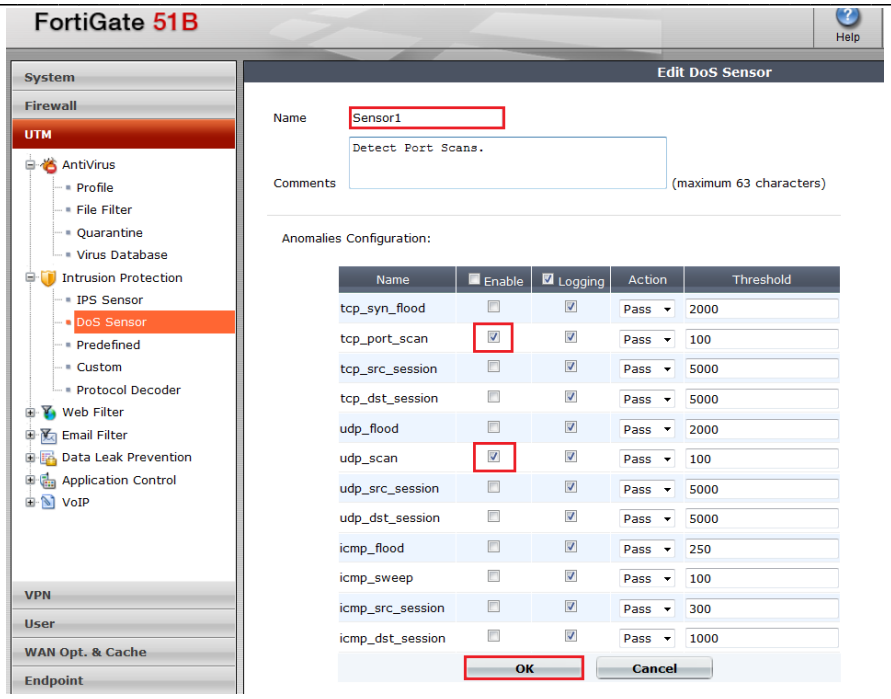


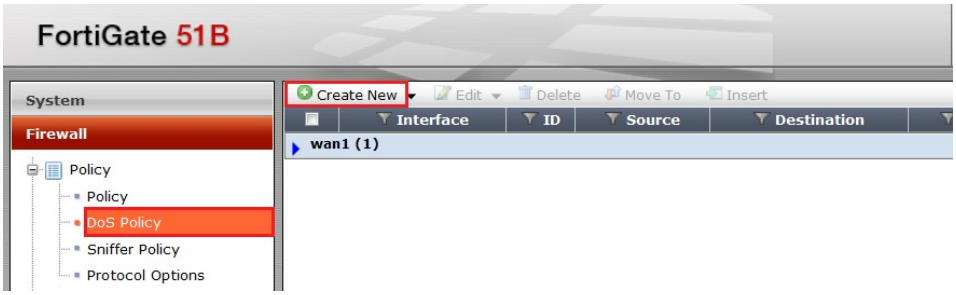


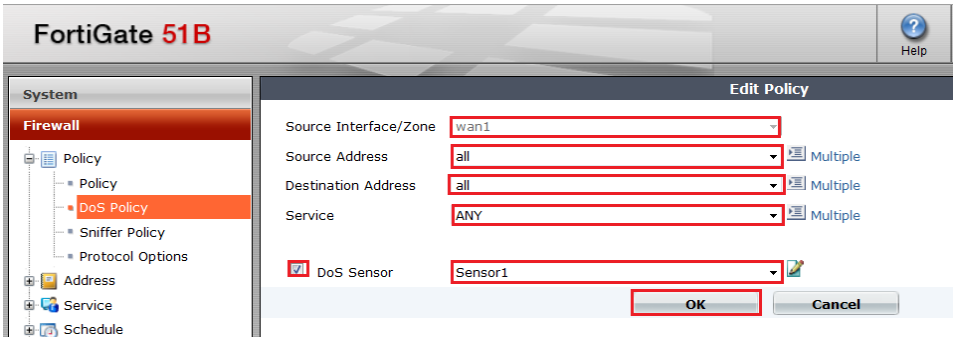


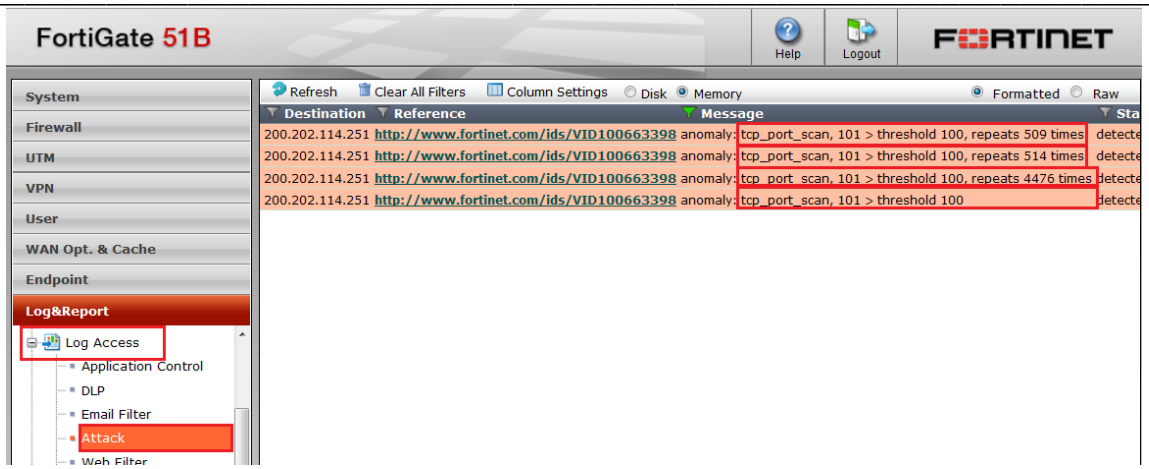
13.3 Port Scan



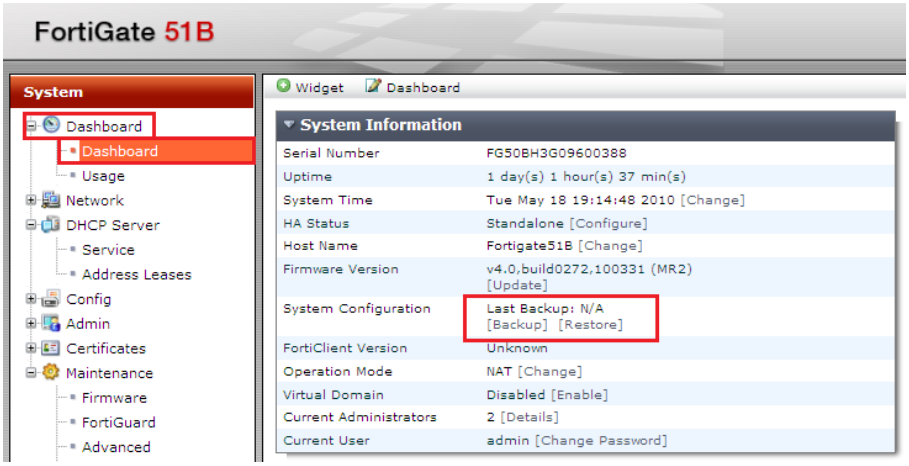

FortiGate 51B
Help
System
Firewall
UTM
AntiVirus
Profile
File Filter
Quarantine
Virus Database
Intrusion Protection
IPS Sensor
DoS Sensor
Predefined
Custom
Protocol Decoder
Web Filter
Email Filter
Data Leak Prevention
Application Control
VoIP
VPN
User
WAN Opt. & Cache
Endpoint
Edit DoS Sensor
Name
Sensor1
Comments
Detect Port Scans.
(maximum 63 characters)
Anomalies Configuration:
Name
Enable
Logging
Action
Threshold
tcp_syn_flood
tcp_port_scan
tcp_src_session
tcp_dst_session
udp_flood
udp_scan
udp_src_session
udp_dst_session
icmp_flood
icmp_sweep
icmp_src_session
icmp_dst_session
Pass
2000
100
5000
5000
2000
100
5000
5000
250
100
300
1000
OK
Cancel

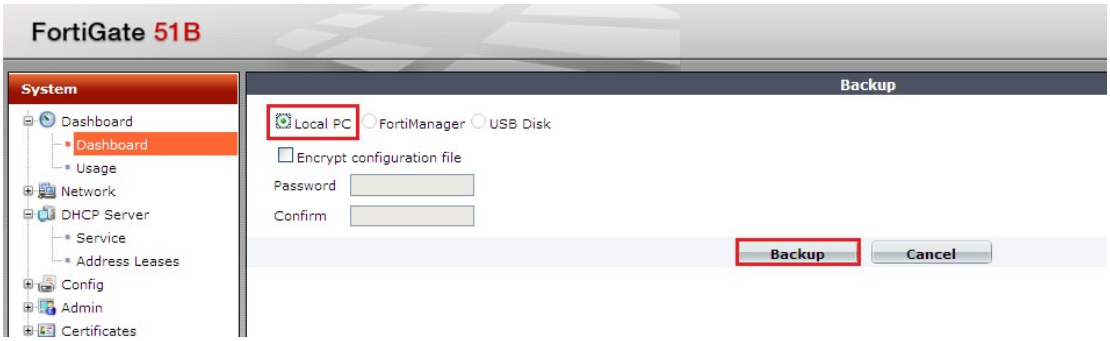

FortiGate 51B
System
Firewall
Policy
Policy
DoS Policy
Sniffer Policy
Protocol Options
Create New
Edit
Delete
Move To
Insert
Interface
ID
Source
Destination
wan1 (1)

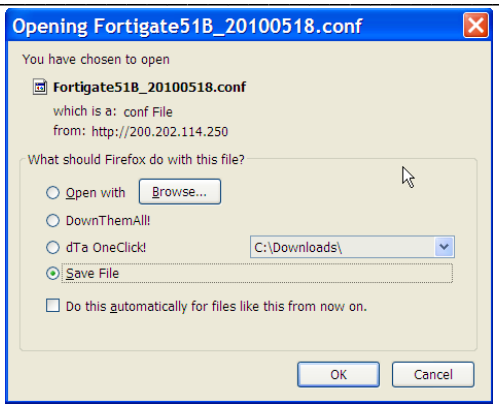

FortiGate 51B
Help
System
Firewall
Policy
Policy
DoS Policy
Sniffer Policy
Protocol Options
Address
Service
Schedule
Edit Policy
Source Interface/Zone
wan1
Source Address
all
Multiple
Destination Address
all
Multiple
Service
ANY
Multiple
DoS Sensor
Sensor1
OK
Cancel



11 Backup e Restore







13.4 Backup Através da CLI

```
Fortigate51B # execute backup full-config tftp my-config.cfg 200.202.114.251
Please wait...
Connect to tftp server 200.202.114.251 ...
#
Send config file to tftp server OK.

Fortigate51B #
```

14 OSPF

As configurações abaixo apresentam a configuração de OSPF via CLI.

14.1 Configuração VIA CLI

```
Fortigate51B # show router ospf
config router ospf
        config area
            edit 0.0.0.0
            next
        end
        config network
            edit 1
                set prefix 200.202.114.248 255.255.255.248
            next
            edit 2
                set prefix 10.123.123.0 255.255.255.0
            next
        end
        config redistribute "connected"
        end
        config redistribute "static"
```

```
        end
        config redistribute "rip"
        end
        config redistribute "bgp"
        end
    set router-id 10.123.123.1
end
```

14.2 Monitoração do OSPF via CLI

14.2.1 Rotas Aprendidas

```
Fortigate51B # get router info ospf route
C  10.123.123.0/24 [10] is directly connected, internal, Area 0.0.0.0
O  172.16.100.0/24 [20] via 10.123.123.100, internal, Area 0.0.0.0
                        via 10.123.123.101, internal, Area 0.0.0.0
O  172.16.101.0/24 [20] via 10.123.123.100, internal, Area 0.0.0.0
                        via 10.123.123.102, internal, Area 0.0.0.0
O  172.16.102.0/24 [20] via 10.123.123.101, internal, Area 0.0.0.0
                        via 10.123.123.102, internal, Area 0.0.0.0
C  200.202.114.248/29 [10] is directly connected, wan1, Area 0.0.0.0
```

14.2.2 Interfaces

```
Fortigate51B # get router info ospf interface
internal is up, line protocol is up
  Internet Address 10.123.123.1/24, Area 0.0.0.0, MTU 1500
  Process ID 0, Router ID 10.123.123.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DROther, Priority 1
  Designated Router (ID) 10.123.123.101, Interface Address 10.123.123.101
  Backup Designated Router (ID) 10.123.123.102, Interface Address 10.123.123.102
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Neighbor Count is 3, Adjacent neighbor count is 2
  Crypt Sequence Number is 525087
  Hello received 374 sent 125, DD received 8 sent 12
  LS-Req received 2 sent 2, LS-Upd received 21 sent 7
  LS-Ack received 11 sent 10, Discarded 8
wan1 is up, line protocol is up
  Internet Address 200.202.114.250/29, Area 0.0.0.0, MTU 1500
  Process ID 0, Router ID 10.123.123.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.123.123.1, Interface Address 200.202.114.250
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Neighbor Count is 0, Adjacent neighbor count is 0
  Crypt Sequence Number is 524390
```

```
  Hello received 0 sent 186, DD received 0 sent 0
  LS-Req received 0 sent 0, LS-Upd received 0 sent 0
  LS-Ack received 0 sent 0, Discarded 0
```

14.2.3 Neighbors

```
Fortigate51B # get router info ospf neighbor

OSPF process 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.123.123.100    1   2-Way/DROther   00:00:32    10.123.123.100  internal
10.123.123.101    1   Full/DR         00:00:36    10.123.123.101  internal
10.123.123.102    1   Full/Backup     00:00:30    10.123.123.102  internal
```

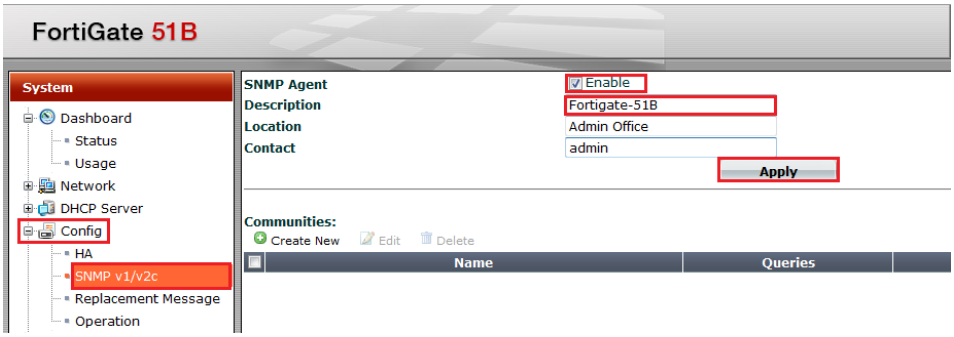
14.2.4 Status

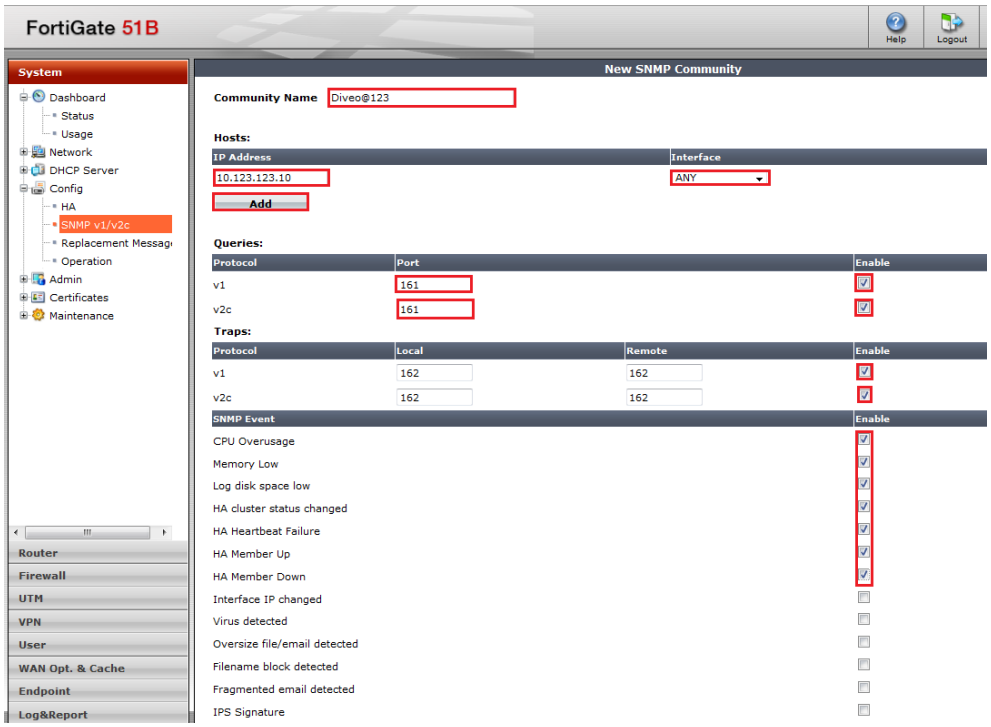
```
Fortigate51B # get router info ospf status
 Routing Process "ospf 0" with ID 10.123.123.1
 Process uptime is 43 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Do not support Restarting
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Refresh timer 10 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 1
 Number of LSA received 26
 Number of areas attached to this router: 1
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 2(2)
        Number of fully adjacent neighbors in this area is 2
        Area has no authentication
        SPF algorithm last executed 00:21:27.340 ago
        SPF algorithm executed 10 times
        Number of LSA 8. Checksum 0x026725
```

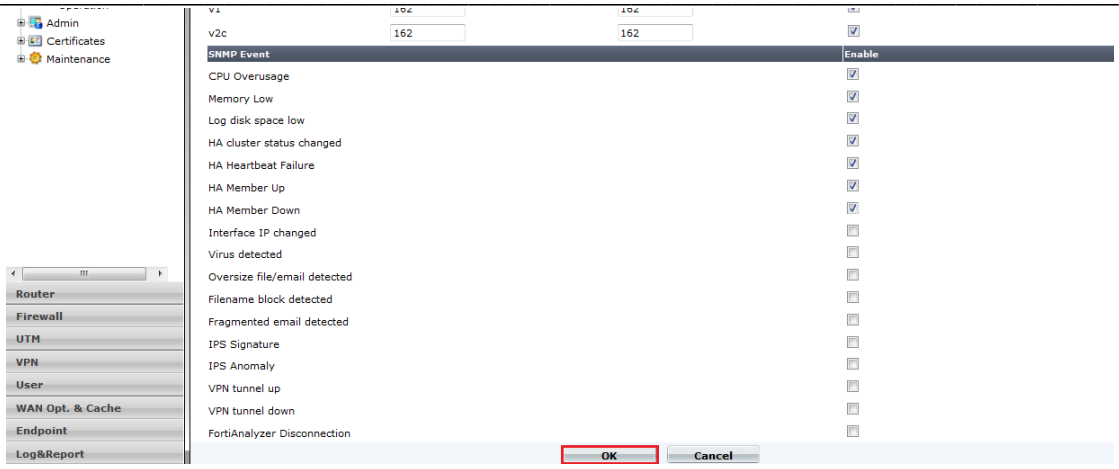
14.2.5 Executar Clear no Processo OSPF

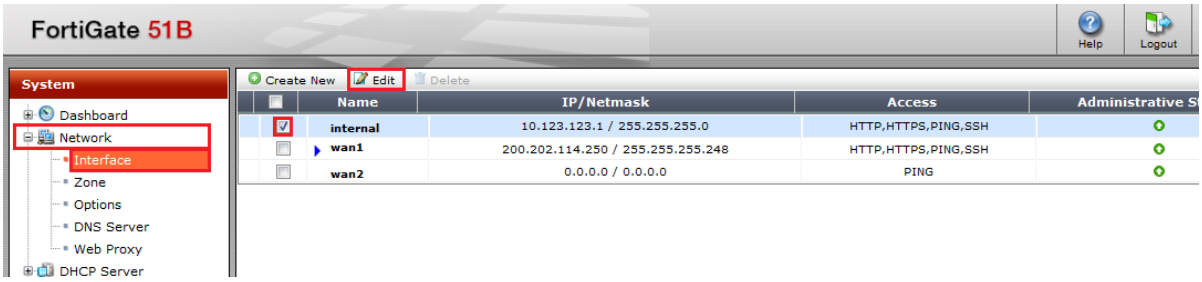
```
Fortigate51B # execute router clear ospf process
```

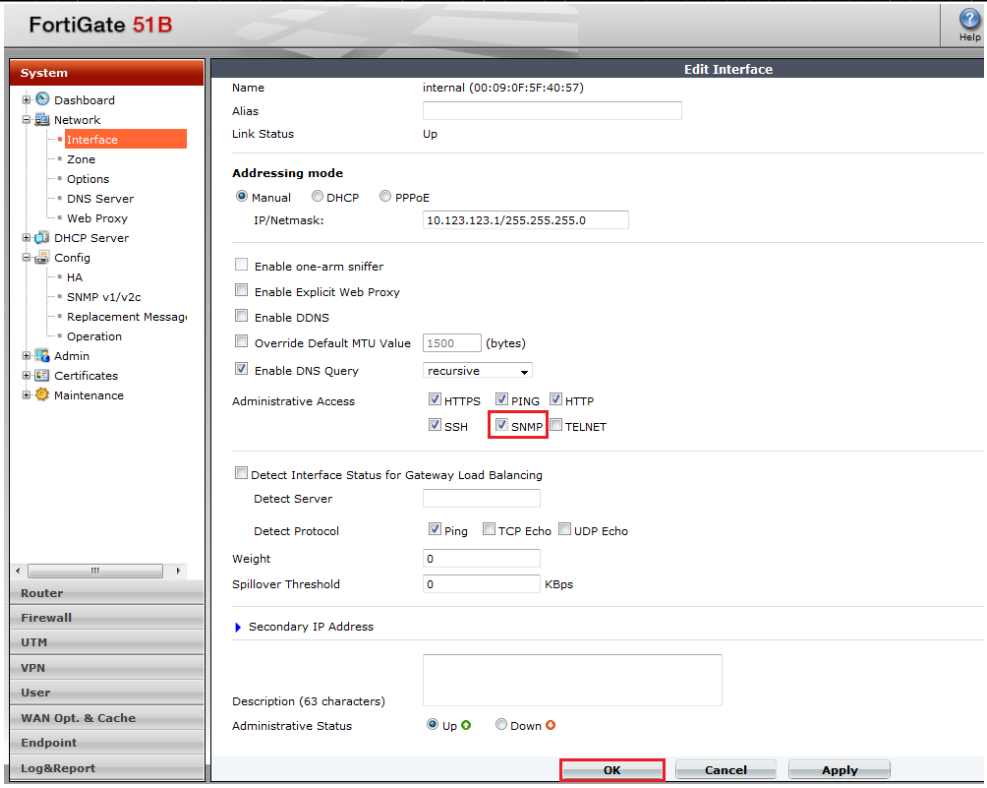
15 SNMP


FortiGate 51B
System
Dashboard
Status
Usage
Network
DHCP Server
Config
HA
SNMP v1/v2c
Replacement Message
Operation
SNMP Agent
Enable
Description
Fortigate-51B
Location
Admin Office
Contact
admin
Apply
Communities:
Create New
Edit
Delete
Name
Queries


FortiGate 51B
Help
Logout
System
Dashboard
Status
Usage
Network
DHCP Server
Config
HA
SNMP v1/v2c
Replacement Messag
Operation
Admin
Certificates
Maintenance
Router
Firewall
UTM
VPN
User
WAN Opt. & Cache
Endpoint
Log&Report
New SNMP Community
Community Name
Diveo@123
Hosts:
IP Address
Interface
10.123.123.10
ANY
Add
Queries:
Protocol
Port
Enable
v1
161
v2c
161
Traps:
Protocol
Local
Remote
Enable
v1
162
162
v2c
162
162
SNMP Event
Enable
CPU Overusage
Memory Low
Log disk space low
HA cluster status changed
HA Heartbeat Failure
HA Member Up
HA Member Down
Interface IP changed
Virus detected
Oversize file/email detected
Filename block detected
Fragmented email detected
IPS Signature


Admin
Certificates
Maintenance
v2c
162
162
SNMP Event
Enable
CPU Overusage
Memory Low
Log disk space low
HA cluster status changed
HA Heartbeat Failure
HA Member Up
HA Member Down
Interface IP changed
Virus detected
Oversize file/email detected
Filename block detected
Fragmented email detected
IPS Signature
IPS Anomaly
VPN tunnel up
VPN tunnel down
FortiAnalyzer Disconnection
Router
Firewall
UTM
VPN
User
WAN Opt. & Cache
Endpoint
Log&Report
OK
Cancel


FortiGate 51B
Help
Logout
System
Dashboard
Network
Interface
Zone
Options
DNS Server
Web Proxy
DHCP Server
Create New
Edit
Delete
Name
IP/Netmask
Access
internal
10.123.123.1 / 255.255.255.0
HTTP,HTTPS,PING,SSH
wan1
200.202.114.250 / 255.255.255.248
HTTP,HTTPS,PING,SSH
wan2
0.0.0.0 / 0.0.0.0
PING



Verificação:

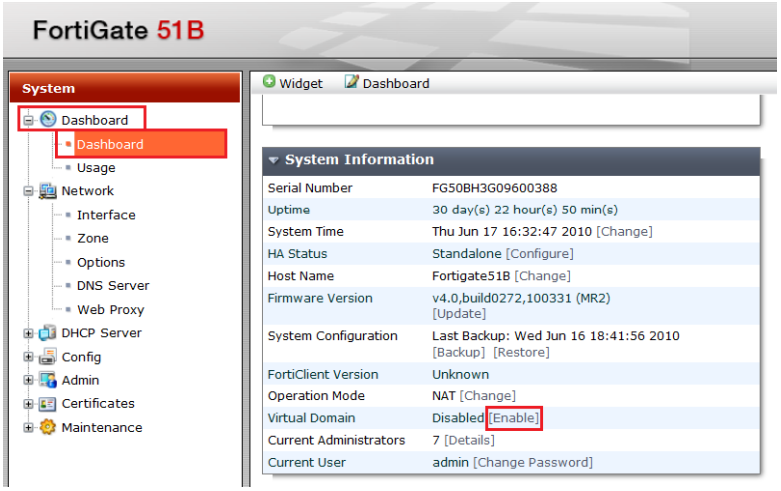
```
root@ServerLab1:/usr/local/src# snmpwalk -c Diveo@123 -v 2c 10.123.123.1 ifDescr
IF-MIB::ifDescr.1 = STRING: internal
IF-MIB::ifDescr.2 = STRING: wan1
IF-MIB::ifDescr.3 = STRING: wan2
IF-MIB::ifDescr.4 = STRING: modem
IF-MIB::ifDescr.5 = STRING: ssl.root
IF-MIB::ifDescr.6 = STRING: MyVPN_Fase1
root@ServerLab1:/usr/local/src# snmpwalk -c Diveo@123 -v 2c 10.123.123.1 ifName
IF-MIB::ifName.1 = STRING: internal
IF-MIB::ifName.2 = STRING: wan1
IF-MIB::ifName.3 = STRING: wan2
IF-MIB::ifName.4 = STRING: modem
IF-MIB::ifName.5 = STRING: ssl.root
IF-MIB::ifName.6 = STRING: MyVPN_Fase1

root@ServerLab1:/usr/local/src# snmpwalk -c Diveo@123 -v 2c 10.123.123.1
ifHCOutOctets
IF-MIB::ifHCOutOctets.1 = Counter64: 54776113946
IF-MIB::ifHCOutOctets.2 = Counter64: 27046002163
IF-MIB::ifHCOutOctets.3 = Counter64: 0
```

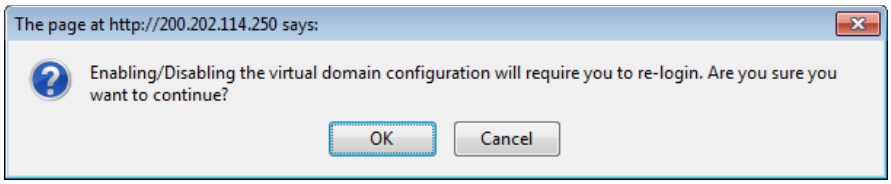
```
IF-MIB::ifHCOutOctets.4 = Counter64: 0
IF-MIB::ifHCOutOctets.5 = Counter64: 236558
IF-MIB::ifHCOutOctets.6 = Counter64: 0
root@ServerLab1:/usr/local/src# snmpwalk -c Diveo@123 -v 2c 10.123.123.1
ifHCInOctets
IF-MIB::ifHCInOctets.1 = Counter64: 25686078927
IF-MIB::ifHCInOctets.2 = Counter64: 27232309330
IF-MIB::ifHCInOctets.3 = Counter64: 0
IF-MIB::ifHCInOctets.4 = Counter64: 0
IF-MIB::ifHCInOctets.5 = Counter64: 256188
IF-MIB::ifHCInOctets.6 = Counter64: 0

root@ServerLab1:/usr/local/src# snmpwalk -c Diveo@123 -v 2c 10.123.123.1
ifOutUcastPkts
IF-MIB::ifOutUcastPkts.1 = Counter32: 293773197
IF-MIB::ifOutUcastPkts.2 = Counter32: 174202249
IF-MIB::ifOutUcastPkts.3 = Counter32: 0
IF-MIB::ifOutUcastPkts.4 = Counter32: 0
IF-MIB::ifOutUcastPkts.5 = Counter32: 1319
IF-MIB::ifOutUcastPkts.6 = Counter32: 0
root@ServerLab1:/usr/local/src# snmpwalk -c Diveo@123 -v 2c 10.123.123.1
ifInUcastPkts
IF-MIB::ifInUcastPkts.1 = Counter32: 173709092
IF-MIB::ifInUcastPkts.2 = Counter32: 258467469
IF-MIB::ifInUcastPkts.3 = Counter32: 0
IF-MIB::ifInUcastPkts.4 = Counter32: 0
IF-MIB::ifInUcastPkts.5 = Counter32: 2600
IF-MIB::ifInUcastPkts.6 = Counter32: 0
```

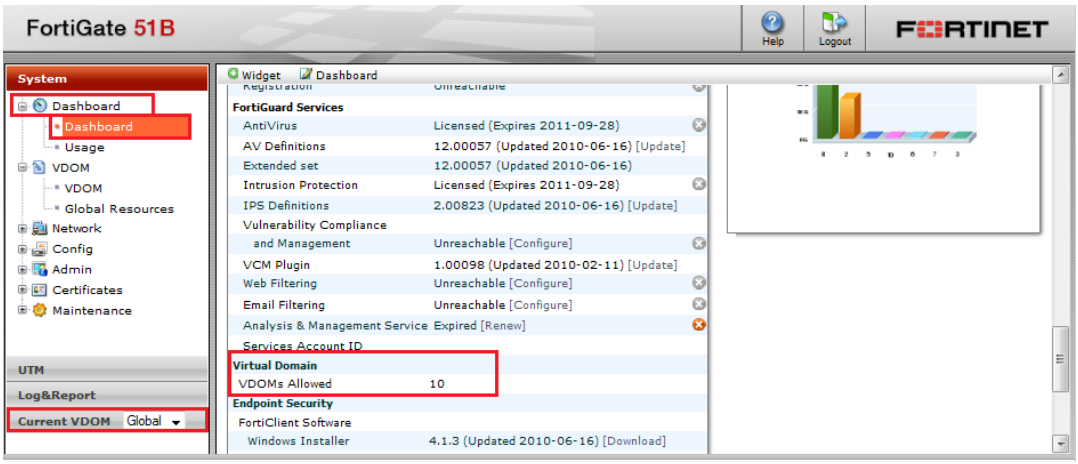
16 VDOM

Através do recurso de Virtual Domain (VDOM) pode-se habilitar as features de virtualização do firewall. O processo de configuração de um VDOM é apresentado nos itens a seguir.

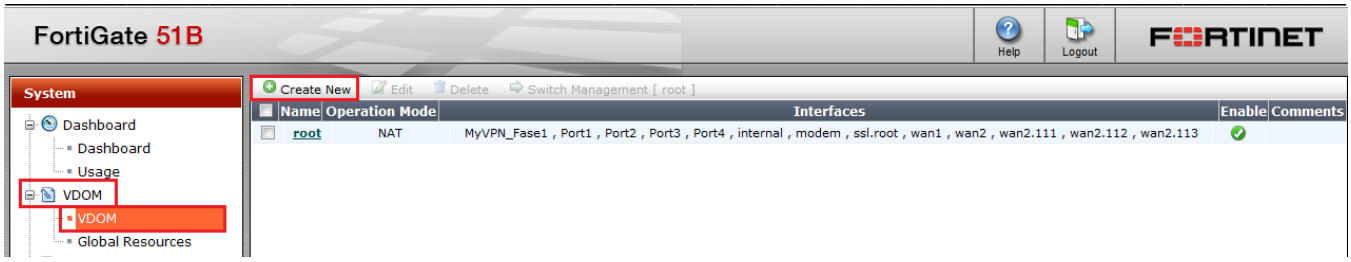
16.1 Habilitar VDOM

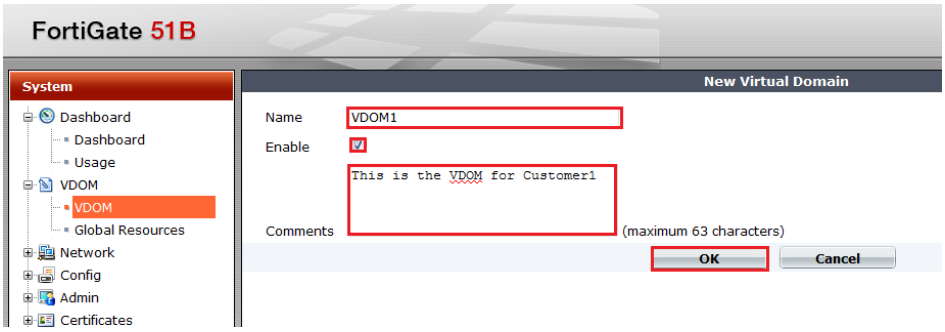


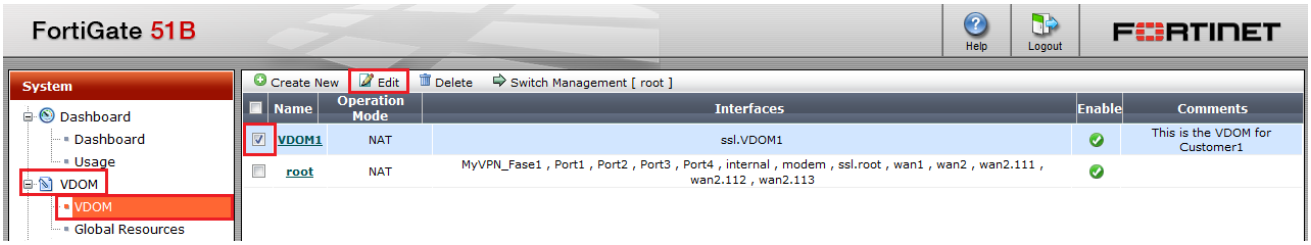




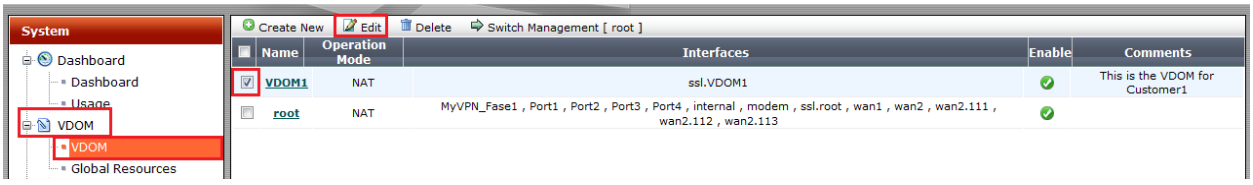
16.2 Criar VDOM

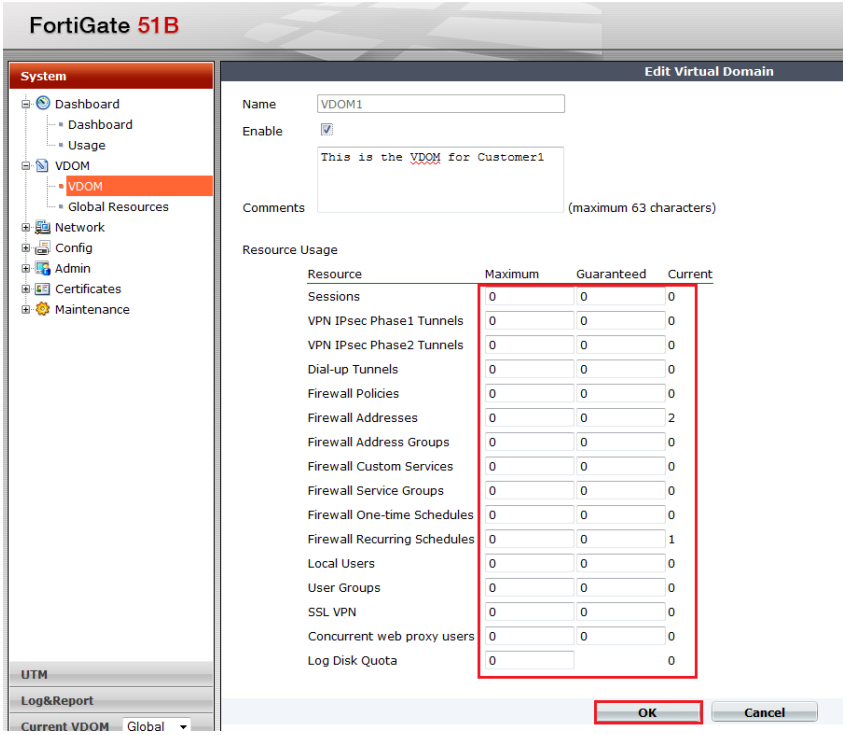






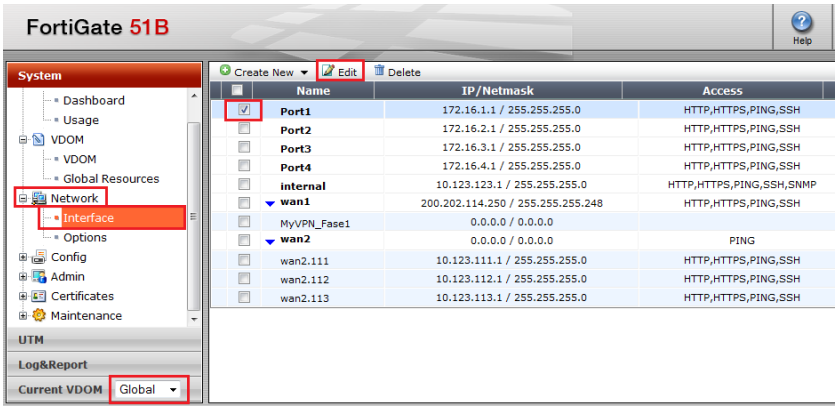
16.3 Editar Limites Para o VDOM

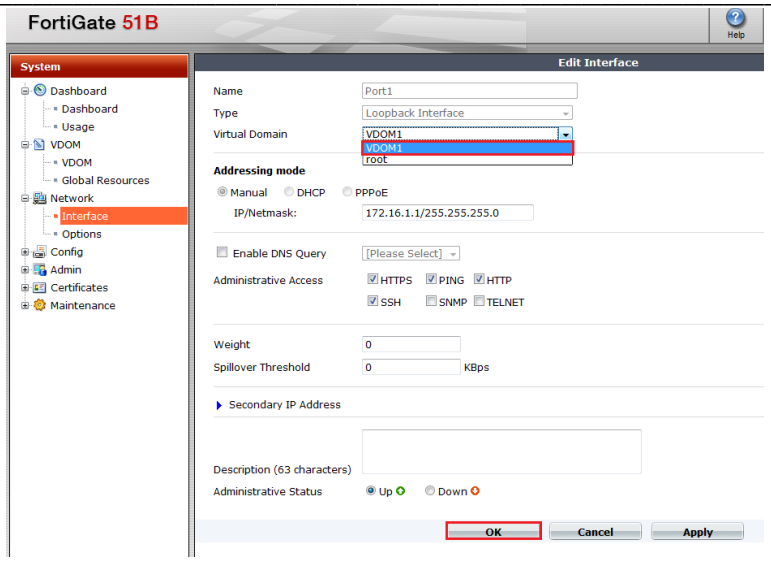




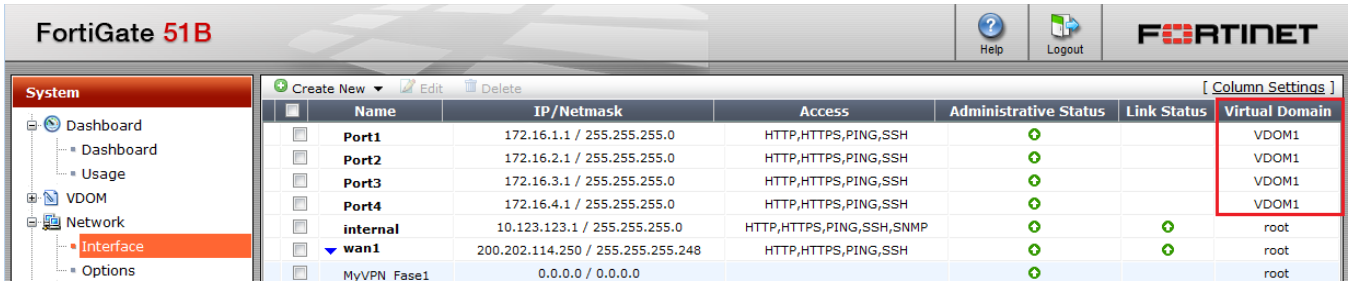
16.4 Adicionar Interfaces ao VDOM

Inicialmente todas as interfaces pertencem ao VDOM Global. Elas devem ser transferidas para o VDOM desejado.

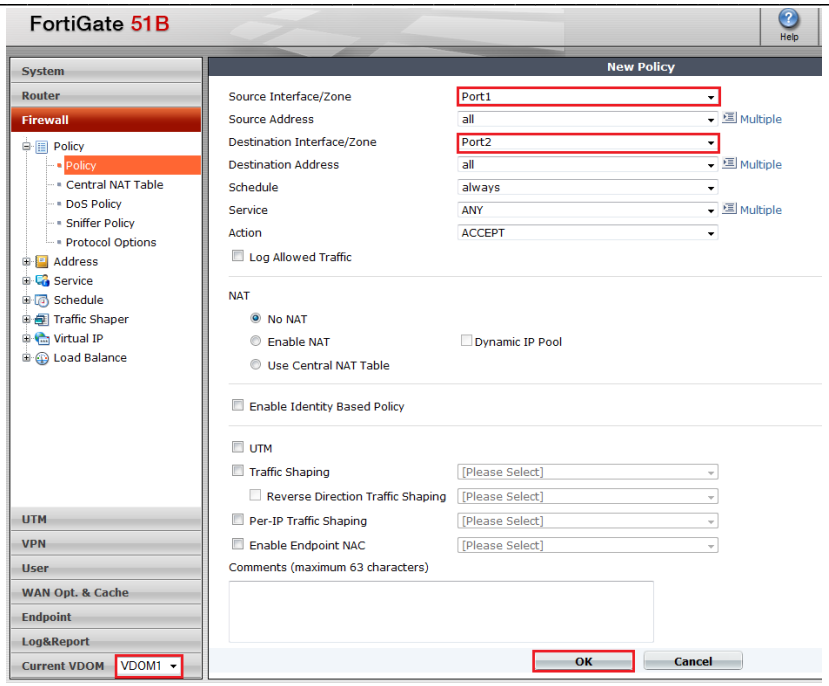




Pode-se ajustar as colunas a serem apresentadas para mostrar a qual interface cada VDOM está relacionado:



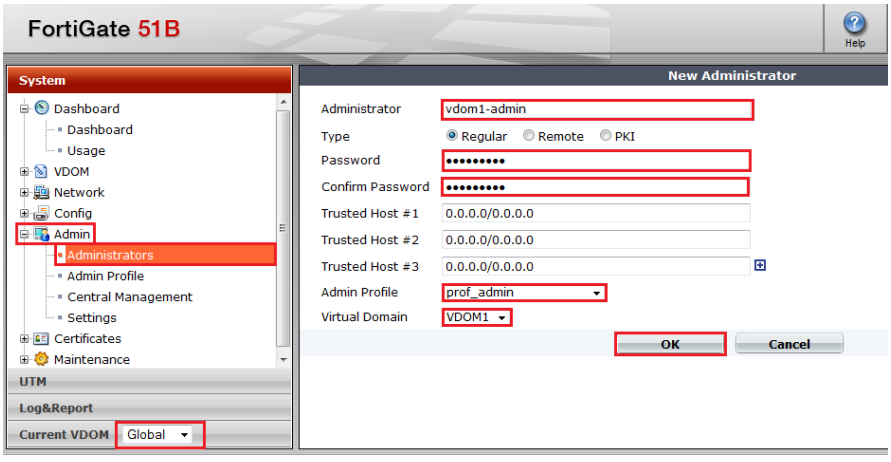
Dentro do VDOM específico não aparecerá a opção Network -> Interface como ocorre no VDOM global. Nos entanto estas portas estarão disponíveis para a configuração das regras de firewall no VDOM específico:



16.5 Adicionar Administradores ao VDOM

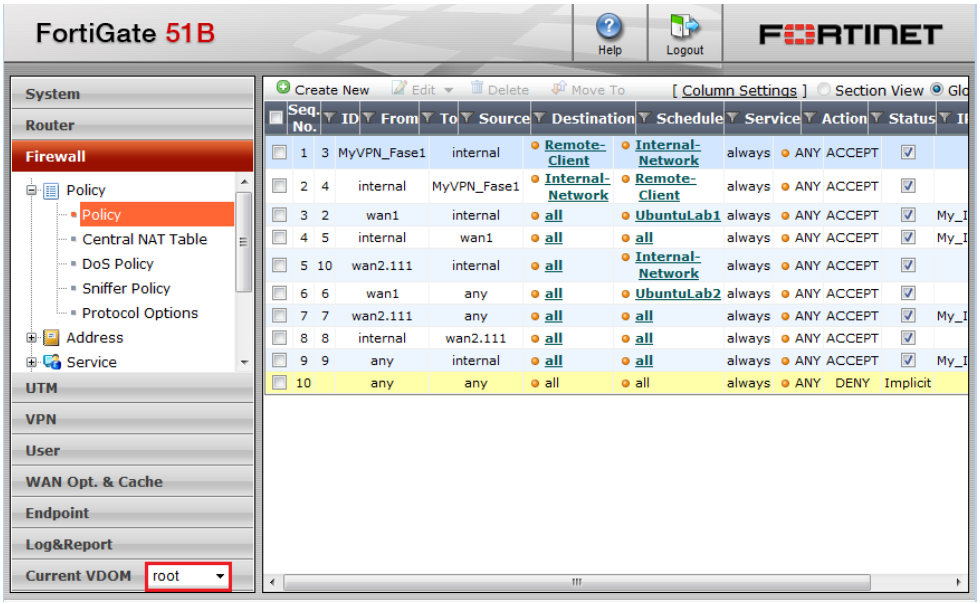
Os administradores definidos no VDOM Global podem configurar todos os VDOMs através da interface web (selecionando-se o VDOM desejado em "Current VDOM").

Pode-se ainda criar administradores específicos para cada VDOM através do VDOM Global:

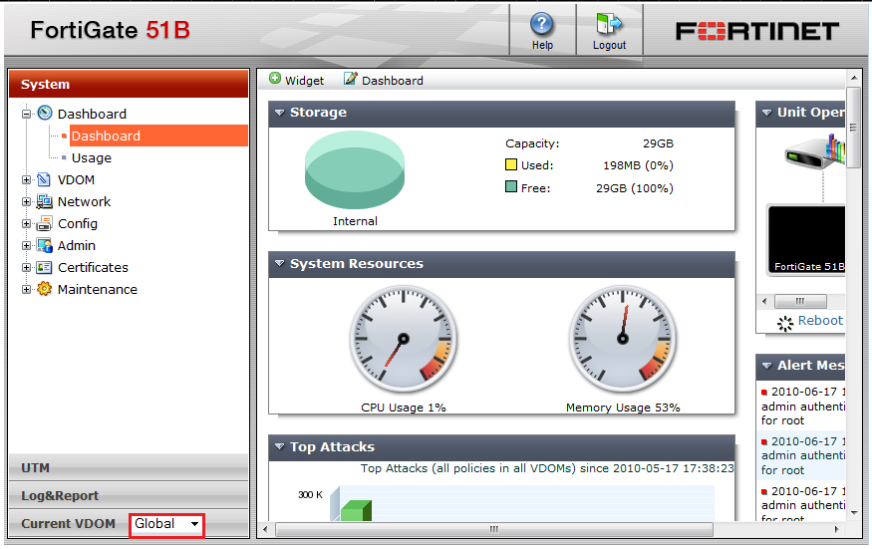


16.6 VDOM Root e VDOM Global

As regras referentes ao Fortigate que não estão associadas a algum VDOM específico devem ser configuradas no VDOM root:

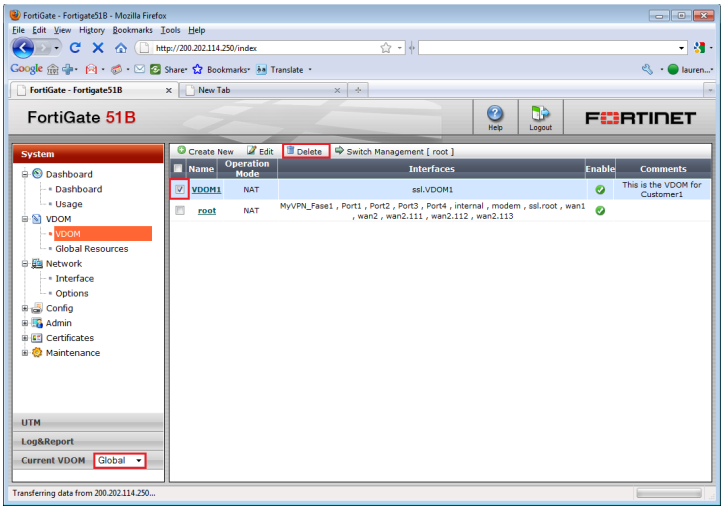


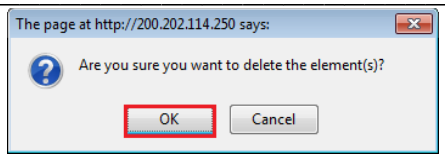
No VDOM Global estarão disponíveis apenas as opções: Dashboard, UTM e Log&Report:



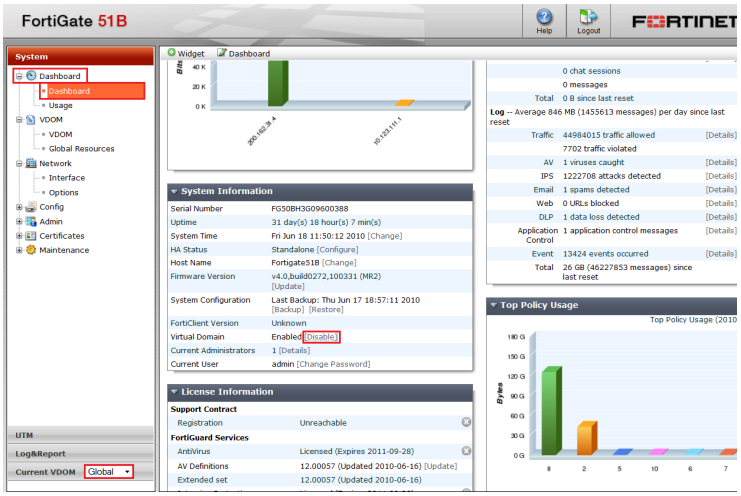
16.7 Remover VDOM

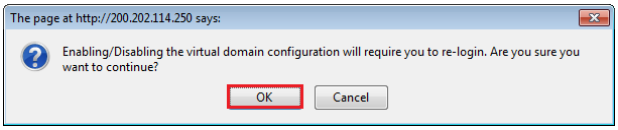
Antes de remover um VDOM todos os objetos que fazem referência a ele devem ser removidos: interfaces, rotas, objetos de firewall (regras, grupos, endereços, etc...), usuários, UTM, VPN, usuários e grupos, logging, DHCP servers e VDOM administrators.





16.8 Desabilitar VDOM





16.9 Command Line – CLI

Quando o FortiGate opera com o modo VDOM habilitado deve-se selecionar o VDOM a ser configurado.

Após o login (via command line) o administrador estará no contexto do VDOM "root".

Para selecionar o domain desejado (Global ou algum outro domain previamente criado) deve-se executar os comandos abaixo:

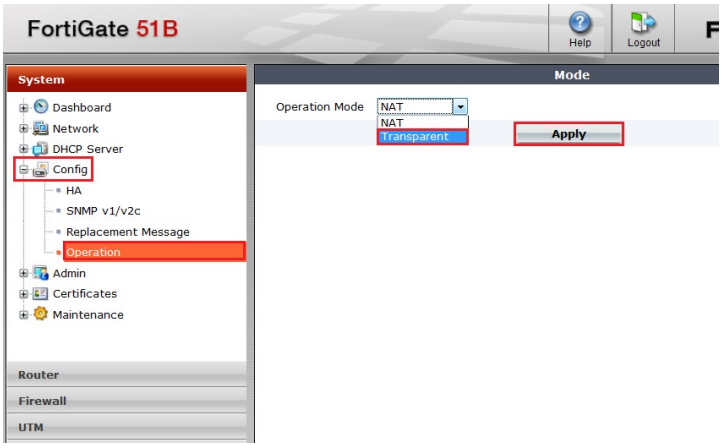
```
FG-VHOST1 # config ?
global     config global
vdom       config vdom
```

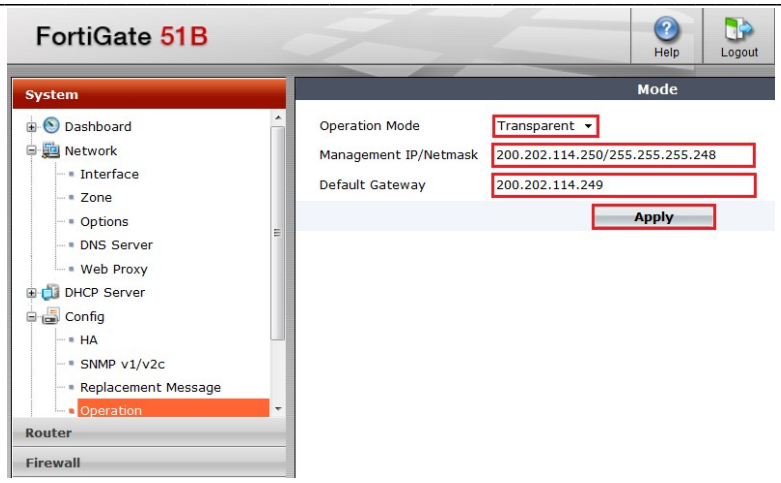
```
FG-VHOST1 # config vdom
FG-VHOST1 (vdom) # edit ?
<vdom>    Virtual Domain Name
VDOM1
VDOM2
VDOM3
Root

FG-VHOST1 (vdom) # edit VDOM1
current vf=VDOM1:3

FG-VHOST1 (VDOM1) #

FG-VHOST1 (VDOM1) # get system session status
The total number of sessions for the current VDOM: 12
```

*Obs: Deve-se usar com cautela o comando "edit VDOM", pois caso seja digitado um VDOM não existente um novo será criado (observar que o nome dos VDOMs diferencia letras maiúsculas de minúsculas).

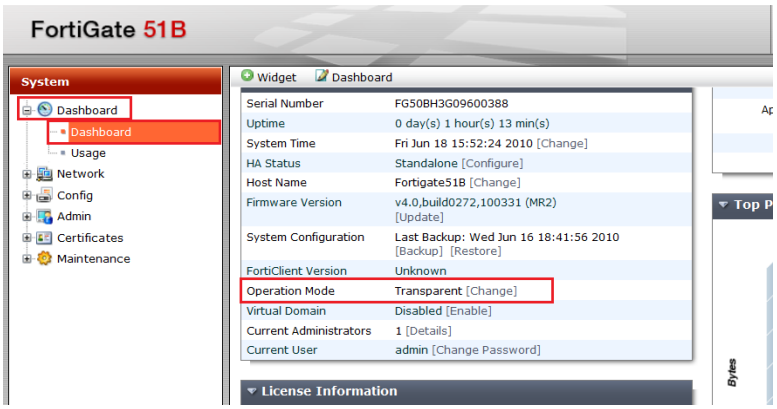
17 Operação no Modo Transparent/Bridge

O Fortigate pode operar no modo transparent/bridge. Neste modo todas as suas interfaces pertecem ao uma mesma camada 2.





*Observação: nos testes de laboratório o equipamento perdeu as configurações de Default Gateway após o apply.



17.1 Spanning Tree

Os BPDUs do Spanning Tree não são encaminhados por default. Para que os BPDUs do Spanning Tree sejam encaminhados deve-se usar o comando "set stpforward enable" (através da CLI) em todas as interfaces que devam realizar o encaminhamento dos pacotes BPDU.

17.2 Multicast

Deve-se criar regras específicas para que os endereços de multicast sejam encaminhados entre interfaces. Por exemplo, para o OSPF deve-se permitir que os pacotes com endereços 224.0.0.5 e 224.0.0.6 sejam liberados em ambos os sentidos.

17.3 Troubleshooting e Best Practices – KB FD30087

O artigo FD30087 do knowledge base da Fortinet apresenta várias orientações referentes ao uso do modo Transparent/Bridge.

http://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD30087&sliceId=1&docTypeID=DT_KCARTICLE_1_1&dialogID=17757534&stateId=0%200%2017755799

Por ser de grande importância para esta questão o referido arqtigo é reproduzido abaixo:

This article gives some configuration best practice and troubleshooting tips for a FortiGate in Transparent mode

Configuration best practice in Transparent mode :

- Spanning tree BPDUs are not forwarded by default ; take care when introducing a FortiGate in the network as L2 loops might be introduced or STP broken.
  To forward spanning tree BPDUs, in CLI use "set stpforward enable" on all interfaces where forwarding is required.

- Use forward domain to forward traffic between only specific interfaces or VLANs and avoid keeping trunks with the default setting (vlan_forward = enabled). This will, for each VLAN, create independent broadcast domains on the FortiGate and confine all broadcasts and multicast traffic between the interfaces belonging to a same forward-domain. As a rule, if there are more than 2 interfaces (VLANs or physical) in a VDOM, always configure different forward_domains on the pairs of interfaces unless you explicitly want to bridge traffic across more than 2 interfaces.
  Another alternative is to create one VDOM per pair of interface/VLAN.

- Only Ethernet II frames forwarded. If IPX or any other protocols in the network which can use different frame types, these are not forwarded by default. For this, the parameter l2forward under the interface configuration has to be enabled.

- In case of multicast traffic in the network passing through FortiGate multicast policies required. For example, you need to set multicast policies if a FortiGate in transparent mode is inserted between 2 OSPF neighbors on a Ethernet segment. In this case, multicast IP 224.0.0.5 and 224.0.0.6 should be allowed for both direction. Same for RIP V2 (224.0.0.9)

- If an out of band management is required, use if possible the VDOM root in NAT mode as management VDOM and create (an) other Transparent mode VDOM(s) for the user traffic.

- If using vlan interfaces in transparent mode, leave the physical interfaces carrying the VLANs on a nat/route VDOM and only associate the required vlan interfaces in the transparent VDOMs.

- If the FortiGate in transparent mode bridges traffic to a router or host using a virtual MAC for one direction and a different physical MAC for the other direction (for instance if VRRP, HSRP protocols are used), it is highly recommended to create a static mac entry in the FortiGate transparent VDOM for the virtual MAC used. This is to make sure the virtual MAC address is known from the transparent mode bridge table. Note: You can only create a static mac entry for interfaces using forward_domain 0 (the default forward-domain).

Troubleshooting steps when facing connectivity problems through a FortiGate in Transparent mode

1 : Check first the L2 MAC address table of the FortiGate

Note : In transparent mode, to forward L2 traffic, the FortiGate does actually rely on its L2 forwarding database, which can be dumped with the command "diag netlink brctl name host root.b" (for the root VDOM), while the ARP table would only be used for it's own IP communications.

The ARP/GARP that are sent by the external devices will be used to populate the L2 FDB and change appropriately the destination MAC addresses for existing sessions in case of MAC changes.

Those commands will dump the L2 forwarding table for each VDOM bridge instance. From there, we should see the devices MAC addresses that are located on each VLAN/VDOM
diag netlink brctl list
diag netlink brctl name host <VDOM_name>.b
Example for the root VDOM :
diag netlink brctl name host root.b

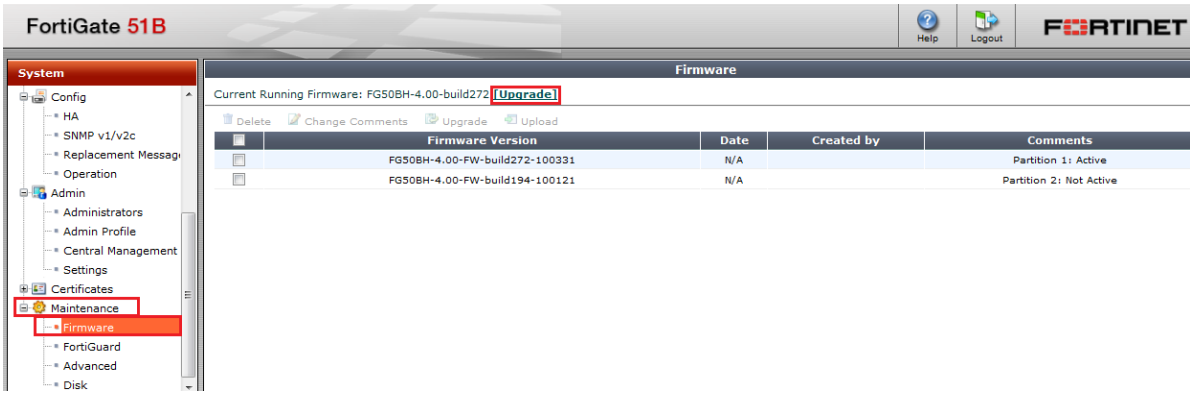
2 - Verify traffic with a sniffer trace:

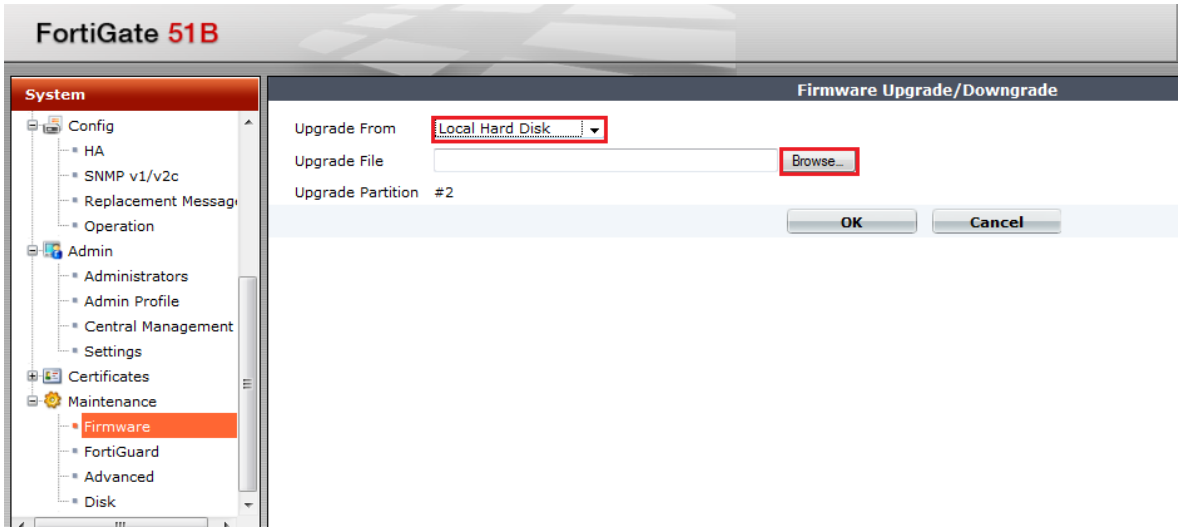
Capture a sniffer trace with the following commands ; run this while making a ping from one device to another device on either side of the FortiGate and while initiating appropriate traffic that exhibits problem. This will tell if the packets are ingressing and egressing the FortiGate. Keep each trace

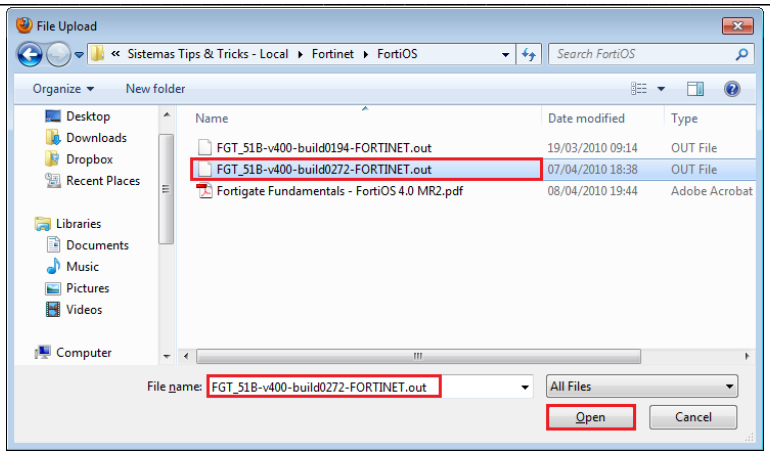
running long enough to get some representative samples.

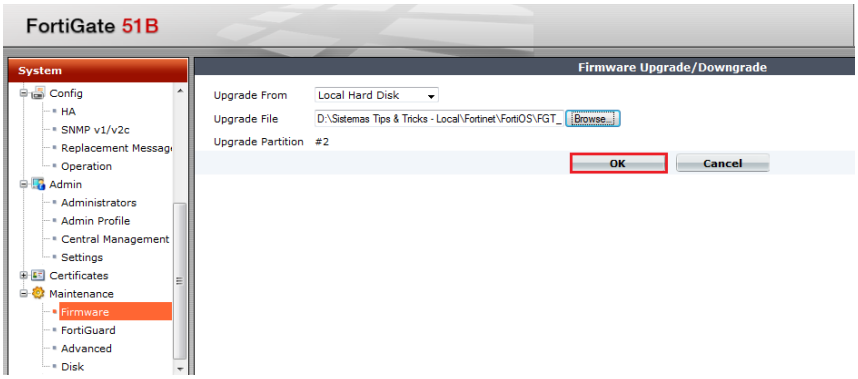
2.1 One global and simultaneous trace
diagnose sniffer packet any "" 4 to stop the sniffer trace, type CTRL+C
2.2 One trace on each port
diagnose sniffer packet portA "" 4
diagnose sniffer packet portB "" 4
etc....
2.3 If applicable, one trace for each VLAN with more verbosity
diagnose sniffer packet <each_vlan_interface> "" 6
3- Debug flow
Capture in each VDOM a "debug flow" trace with the following CLI commands procedure.
Run this while making a ping from one device to another device on either side of the FortiGate and while initiating appropriate traffic that exhibits problem.
This will inform if the traffic is blocked or forwarded and give information about the matching policy.
3.1
==========
diag debug flow filter add <IP_address_of_source_device>
diag debug flow show console enable
diag debug flow show function-name enable
diag debug flow trace start 100
diag debug enable
==========
...to stop the debug, type "diag debug flow trace stop"
3.2
==========
diag debug flow filter add <IP_address_of_destination_device>
diag debug flow show console enable
diag debug flow show function-name enable
diag debug flow trace start 100
diag debug enable
==========
...to stop the debug, type "diag debug flow trace stop"
Example of debug flow output when traffic flows :
id=20085 trace_id=113 msg="vd-tp_mode received a packet(proto=6, 10.160.0.160:4370->10.160.0.152:23) from internal."
id=20085 trace_id=113 msg="Find an existing session, id-00000a40, original direction"
id=20085 trace_id=113 msg="enter fast path"
id=20085 trace_id=113 msg="send out via dev-dmz1, dst-mac-00:01:02:03:04:05"

18 Firmware Upgrade






File Upload
Sistemas Tips & Tricks - Local ▸ Fortinet ▸ FortiOS
Search FortiOS
Organize
New folder
Desktop
Downloads
Dropbox
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Name
Date modified
Type
FGT_51B-v400-build0194-FORTINET.out
19/03/2010 09:14
OUT File
FGT_51B-v400-build0272-FORTINET.out
07/04/2010 18:38
OUT File
Fortigate Fundamentals - FortiOS 4.0 MR2.pdf
08/04/2010 19:44
Adobe Acrobat
File name: FGT_51B-v400-build0272-FORTINET.out
All Files
Open
Cancel


FortiGate 51B
System
Config
HA
SNMP v1/v2c
Replacement Messag
Operation
Admin
Administrators
Admin Profile
Central Management
Settings
Certificates
Maintenance
Firmware
FortiGuard
Advanced
Disk
Firmware Upgrade/Downgrade
Upgrade From
Local Hard Disk
Upgrade File
D:\Sistemas Tips & Tricks - Local\Fortinet\FortiOS\FGT_
Browse...
Upgrade Partition
#2
OK
Cancel

19 Performance

19.1 Ping Flood

Teste:

- IP de origem de origem e destinos fixos;
- Intervalos de entre pacotes: 100ms e 300ms;
- Tamanho dos pacostes: 100, 500 e 1400 bytes.

Ping Flood							
Pkt Size	Taxa (pkt/s)			Banda (kbps)			CPU Util. 1 min (%)
	IN	OUT	Total	IN	OUT	Total	
100	8.231	8.230	16.461	9.347	9.346	18.693	96
100	3.015	3.015	6.030	3.425	3.426	6.851	43
500	8.045	8.045	16.090	34.936	34.934	69.870	98
500	3.081	3.081	6.162	13.373	13.367	26.740	43
1400	4.368	4.368	8.736	50.459	50.453	100.912	72
1400	3.055	3.055	6.110	34.242	30.240	64.482	55

19.2 IPerf

Teste:

- 100 sessões TCP;
- 200 sessões UDP.

IPerf			
Protocolo	Sessões	Banda (Kbps)	CPU Util. 1 min (%)
TCP	100	98.451	75
UDP	200	64.453	55

19.3 Web Attack

Teste:

- Simulação de ataque através da ferramenta Nikto;
- Os ataques simulados são destinados ao serviço HTTP do alvo;
- Foram geradas várias instâncias do Nikto para aumentar a intensidade dos ataques.

Web Attack (Nikto)		
Sessões	Banda (Kbps)	CPU Util. 1 min (%)
4.935	927	86
9.664	1.712	87
10.577	1.890	85
11.436	2.053	98
28.247	2.055	99

***Observação:** mesmo quando a CPU atingiu 99% de utilização não foi verificado degradação no tempo de acesso HTTP ao servidor alvo do ataque.

19.4 Syn Flood – IP Fixo no Atacante

Teste:

- Simulação de ataque através da ferramenta hping3;
- Os ataques simulados são destinados ao serviço HTTP do alvo;
- Taxa de bloqueio ajustada para 500 pacotes de syn/s provenientes de um memo endereço.

Syn Flood - IP Fixo no Atacante - Taxa de bloqueio = 500 pkt/s		
Taxa (pkts)	Banda (Kbps)	CPU Util. 1 min (%)
991	457	2
7.445	3.195	18
12.090	5.541	55
37.881	12.863	99

19.5 Syn Flood – Spoofed Address no Atacante – Sem Limite de Sessões

Teste:

- Simulação de ataque através da ferramenta hping3;
- Os ataques simulados são destinados ao serviço HTTP do alvo;
- O endereço do atacante variou aleatoriamente (spoofed);
- Sem limite de sessões para um determinado endereço destino ou restrições de taxa de syn.

Syn Flood - IP "spoofado" no Atacante - Sem limite de sessões para destino			
Taxa (pkts)	Banda (Kbps)	Sessões	CPU Util. 1 min (%)
3.234	1.550	5.983	43
4.487	2.180	7.603	77
6.181	2.864	12.615	99

19.6 Syn Flood – Spoofed Address no Atacante – Com Limite de Sessões

Teste:

- Simulação de ataque através da ferramenta hping3;
- Os ataques simulados são destinados ao serviço HTTP do alvo;
- O endereço do atacante variou aleatoriamente (spoofed);
- Limite de sessões ajustado para 2.000 sessões para um determinado endereço de destino.
- Sem restrições para a taxa de syn gerada por um atacante.

Syn Flood - IP "spoofado" no Atacante - Limite de sessões = 2000 por endereço destino			
Taxa (pkts)	Banda (Kbps)	Sessões	CPU Util. 1 min (%)
1.687	619	2.011	7
2.038	1.056	2.012	16
3.500	1.620	2.012	26
5.942	2.630	2.009	48
8.665	3.363	2.009	61
9.167	4.034	2.009	70
13.134	5.711	2.009	90

***Observação1:** Quando o limite de sessões para o servidor alvo foi atingido todos os acessos HTTP para este servidor também falharam.

***Observação2:** Mesmo quando o limite de sessões para o servidor alvo foi atingido (no serviço HTTP) outros serviços entre atacante e alvo continuaram a funcionar (ex: sessões ssh do atacante para o alvo continuaram a ser estabelecidas).

***Observação3:** Quando o serviço definido na DoS Policy foi alterado de HTTP para Any o acesso a qualquer serviço foi interrompido, quando o limite de sessões foi atingido.

20 Troubleshooting

20.1 Ping Extendido

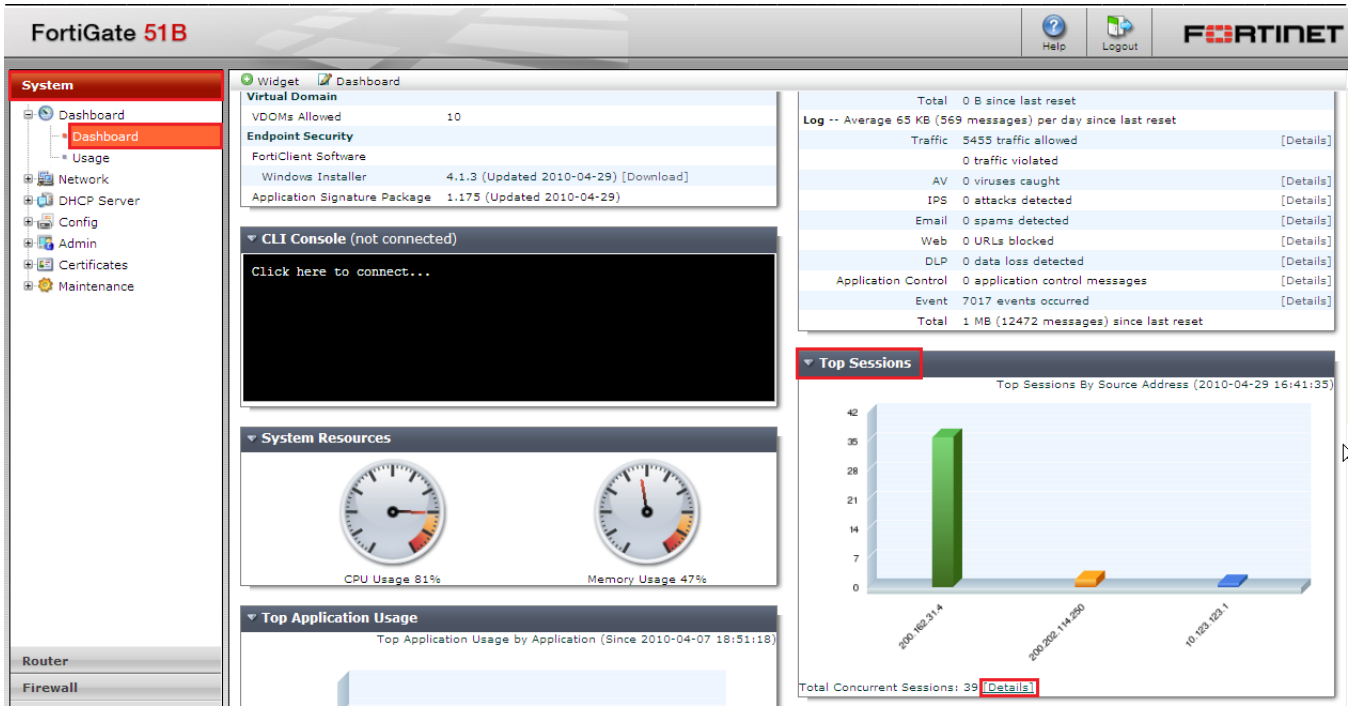
```
Fortigate51B # execute ping-options source 10.123.123.1
Fortigate51B # execute ping-options data-size 1000
Fortigate51B # execute ping-options view-settings
Ping Options:
        Repeat Count: 5
        Data Size: 1000
        Timeout: 2
        Interval: 1
        TTL: 64
        TOS: 0
        DF bit: unset
        Source Address: 10.123.123.1
        Pattern:
        Pattern Size in Bytes: 0
        Validate Reply: no

Fortigate51B # execute ping 10.123.123.10
PING 10.123.123.10 (10.123.123.10): 1000 data bytes
1008 bytes from 10.123.123.10: icmp_seq=0 ttl=255 time=0.2 ms
1008 bytes from 10.123.123.10: icmp_seq=1 ttl=255 time=0.1 ms
1008 bytes from 10.123.123.10: icmp_seq=2 ttl=255 time=0.2 ms
1008 bytes from 10.123.123.10: icmp_seq=3 ttl=255 time=0.2 ms
1008 bytes from 10.123.123.10: icmp_seq=4 ttl=255 time=0.2 ms

--- 10.123.123.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.5/0.5/0.6 ms
```

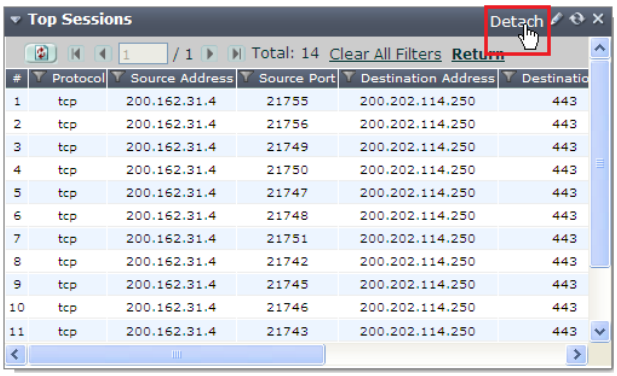
20.2 Captura de Pacotes

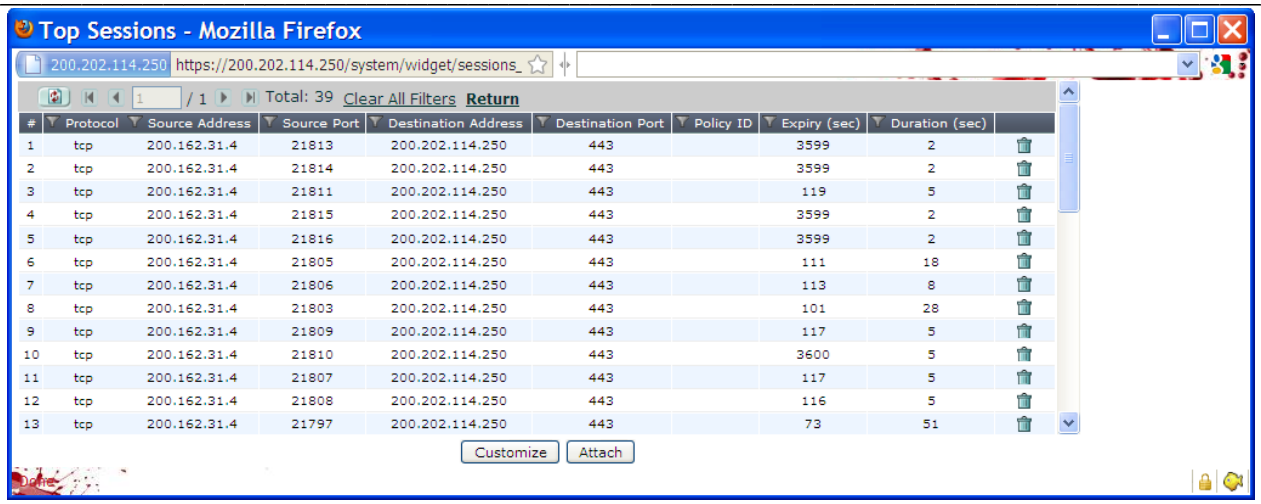
```
FG50BH3G09600388 # diagnose sniffer packet wan1
```

```
<filter>    flexible logical filters for sniffer (or "none").
For example:  To print udp 1812 traffic between forti1 and either forti2 or forti3
'udp and port 1812 and host forti1 and \( forti2 or forti3 \)'

FG50BH3G09600388 # diagnose sniffer packet wan1
interfaces=[wan1]
filters=[none]
0.255837 arp who-has 10.10.4.150 tell 10.10.4.178
0.446700 10.10.4.72 -> 224.0.0.18:  ip-proto-112 20
0.483236 10.10.4.4.137 -> 10.10.7.255.137: udp 50
0.548005 arp who-has 169.254.90.170 (0:1c:58:9:25:cf) tell 10.10.4.30
0.701086 arp who-has 10.10.4.15 (ff:ff:ff:ff:ff:ff) tell 10.10.5.212
0.732879 10.10.4.4.137 -> 10.10.7.255.137: udp 50
0.740086 10.10.6.49.1024 -> 216.156.209.26.53: udp 64
0.837795 arp who-has 10.10.4.20 tell 10.10.4.73
0.873587 10.10.4.4.137 -> 10.10.7.255.137: udp 50
0.874668 10.10.4.4.137 -> 10.10.7.255.137: udp 50
0.936271 stp 802.1d, config, flags [topology change], bridge-id
8000.00:03:e3:4e:61:00.803e
1.218327 arp who-has 10.10.4.39 tell 10.10.4.6
1.219132 10.10.4.39.42942 -> 10.10.4.81.137: udp 50
1.219255 arp who-has 10.10.4.39 tell 10.10.4.81
1.220101 10.10.4.39.42943 -> 10.10.4.125.137: udp 50
1.220211 arp who-has 10.10.4.39 tell 10.10.4.125
1.233430 10.10.4.4.137 -> 10.10.7.255.137: udp 50
1.245205 10.10.6.107.137 -> 10.10.7.255.137: udp 50
1.396638 1.1.1.1.123 -> 10.70.4.25.123: udp 48
1.396729 192.168.1.101.123 -> 10.70.4.25.123: udp 48
1.396820 192.168.56.
24 packets received by filter
0 packets dropped by kernel
```

20.3 Listar Sessões


FortiGate 51B
Help
Logout
FORTINET
System
Dashboard
Dashboard
Usage
Network
DHCP Server
Config
Admin
Certificates
Maintenance
Router
Firewall
Widget
Dashboard
Virtual Domain
VDOMs Allowed 10
Endpoint Security
FortiClient Software
Windows Installer 4.1.3 (Updated 2010-04-29) [Download]
Application Signature Package 1.175 (Updated 2010-04-29)
CLI Console (not connected)
Click here to connect...
System Resources
CPU Usage 81%
Memory Usage 47%
Top Application Usage
Top Application Usage by Application (Since 2010-04-07 18:51:18)
Total 0 B since last reset
Log -- Average 65 KB (569 messages) per day since last reset
Traffic 5455 traffic allowed [Details]
0 traffic violated
AV 0 viruses caught [Details]
IPS 0 attacks detected [Details]
Email 0 spams detected [Details]
Web 0 URLs blocked [Details]
DLP 0 data loss detected [Details]
Application Control 0 application control messages [Details]
Event 7017 events occurred [Details]
Total 1 MB (12472 messages) since last reset
Top Sessions
Top Sessions By Source Address (2010-04-29 16:41:35)
42
35
28
21
14
7
0
200.162.31.4
200.202.114.250
10.123.123.1
Total Concurrent Sessions: 39 [Details]


Top Sessions
Detach
1 / 1 Total: 14 Clear All Filters Return
Protocol Source Address Source Port Destination Address Destinatio
1 tcp 200.162.31.4 21755 200.202.114.250 443
2 tcp 200.162.31.4 21756 200.202.114.250 443
3 tcp 200.162.31.4 21749 200.202.114.250 443
4 tcp 200.162.31.4 21750 200.202.114.250 443
5 tcp 200.162.31.4 21747 200.202.114.250 443
6 tcp 200.162.31.4 21748 200.202.114.250 443
7 tcp 200.162.31.4 21751 200.202.114.250 443
8 tcp 200.162.31.4 21742 200.202.114.250 443
9 tcp 200.162.31.4 21745 200.202.114.250 443
10 tcp 200.162.31.4 21746 200.202.114.250 443
11 tcp 200.162.31.4 21743 200.202.114.250 443



#	Protocol	Source Address	Source Port	Destination Address	Destination Port	Policy ID	Expiry (sec)	Duration (sec)
1	tcp	200.162.31.4	21813	200.202.114.250	443		3599	2
2	tcp	200.162.31.4	21814	200.202.114.250	443		3599	2
3	tcp	200.162.31.4	21811	200.202.114.250	443		119	5
4	tcp	200.162.31.4	21815	200.202.114.250	443		3599	2
5	tcp	200.162.31.4	21816	200.202.114.250	443		3599	2
6	tcp	200.162.31.4	21805	200.202.114.250	443		111	18
7	tcp	200.162.31.4	21806	200.202.114.250	443		113	8
8	tcp	200.162.31.4	21803	200.202.114.250	443		101	28
9	tcp	200.162.31.4	21809	200.202.114.250	443		117	5
10	tcp	200.162.31.4	21810	200.202.114.250	443		3600	5
11	tcp	200.162.31.4	21807	200.202.114.250	443		117	5
12	tcp	200.162.31.4	21808	200.202.114.250	443		116	5
13	tcp	200.162.31.4	21797	200.202.114.250	443		73	51

20.4 Debug de IPSec VPN

```
Fortigate51B # diagnose debug enable
Fortigate51B # diagnose debug console timestamp enable
Fortigate51B # diagnose debug application ike -1
Fortigate51B #
2010-05-24 19:28:12 ike 0: comes 200.162.31.4:18831-
>200.202.114.250:500,ifindex=5....
2010-05-24 19:28:12 ike 0: IKEv1 exchange=Aggressive
id=5a09da2104a8bea5/0000000000000000 len=512
2010-05-24 19:28:12 ike 0:MyVPN_Fase1: new connection.
2010-05-24 19:28:12 ike 0:MyVPN_Fase1:39: responder: aggressive mode get 1st
message...
2010-05-24 19:28:12 ike 0:MyVPN_Fase1:39: VID DPD AFCAD71368A1F1C96B8696FC77570100
2010-05-24 19:28:12 ike 0:MyVPN_Fase1:39: DPD negotiated
2010-05-24 19:28:12 ike 0:MyVPN_Fase1:39: VID unknown (16):
AFCA071368A1F1C96B8696FC77570100
2010-05-24 19:28:12 ike 0:MyVPN_Fase1:39: VID forticlient 1.0
6EF67E6852CF311713E50B8B005DB7B8
2010-05-24 19:28:12 ike 0:MyVPN_Fase1:39: VID draft-ietf-ipsec-nat-t-ike-03
7D9419A65310CA6F2C179D9215529D56
2010-05-24 19:28:12 ike 0:MyVPN_Fase1:39: VID draft-ietf-ipsec-nat-t-ike-00
4485152D18B6BBCD0BE8A8469579DDCC
2010-05-24 19:28:12 ike 0:MyVPN_Fase1:39: negotiation result
2010-05-24 19:28:12 ike 0:MyVPN_Fase1:39: proposal id = 1:
2010-05-24 19:28:12 ike 0:MyVPN_Fase1:39:   protocol id = ISAKMP:
2010-05-24 19:28:12 ike 0:MyVPN_Fase1:39:      trans_id = KEY_IKE.
2010-05-24 19:28:12 ike 0:MyVPN_Fase1:39:      encapsulation = IKE/none
2010-05-24 19:28:12 ike 0:MyVPN_Fase1:39:         type=OAKLEY_ENCRYPT_ALG,
val=3DES_CBC.
2010-05-24 19:28:12 ike 0:MyVPN_Fase1:39:         type=OAKLEY_HASH_ALG, val=MD5.
```

```
2010-05-24 19:28:12 ike 0:MyVPN_Fase1:39:         type=AUTH_METHOD,
val=PRESHARED_KEY.
2010-05-24 19:28:12 ike 0:MyVPN_Fase1:39:         type=OAKLEY_GROUP, val=1536.
2010-05-24 19:28:12 ike 0:MyVPN_Fase1:39: ISKAMP SA lifetime=28800
2010-05-24 19:28:12 ike 0:MyVPN_Fase1:39: selected NAT-T version: draft-ietf-ipsec-
nat-t-ike-03
2010-05-24 19:28:12 ike 0:MyVPN_Fase1:39: put connection to natt
list...ip=200.162.31.4.

Fortigate51B # diagnose debug disable
```

20.5 Debug de Sessões

Exemplo de debug de sessões originadas por 200.189.190.105:

```
Fortigate51B # diag debug enable
Fortigate51B # diagnose debug flow filter saddr 200.189.190.105
Fortigate51B # diagnose debug flow show console enable
Fortigate51B # diagnose debug flow trace start 10

Fortigate51B # 2010-06-09 16:02:28 id=36870 trace_id=21 msg="vd-root received a
packet(proto=6, 200.189.190.105:53489->200.202.114.251:80) from wan1."
2010-06-09 16:02:28 id=36870 trace_id=21 msg="allocate a new session-028feeaf"
2010-06-09 16:02:28 id=36870 trace_id=21 msg="find SNAT: IP-10.123.123.10(from
IPPOOL), port-80"
2010-06-09 16:02:28 id=36870 trace_id=21 msg="VIP-10.123.123.10:80, outdev-wan1"
2010-06-09 16:02:28 id=36870 trace_id=21 msg="DNAT 200.202.114.251:80-
>10.123.123.10:80"
2010-06-09 16:02:28 id=36870 trace_id=21 msg="find a route: gw-10.123.123.10 via
internal"
2010-06-09 16:02:28 id=36870 trace_id=21 msg="Allowed by Policy-2:"
2010-06-09 16:02:28 id=36870 trace_id=21 msg="send to ips"
2010-06-09 16:02:28 id=36870 trace_id=22 msg="vd-root received a packet(proto=6,
200.189.190.105:53489->200.202.114.251:80) from wan1."
2010-06-09 16:02:28 id=36870 trace_id=22 msg="Find an existing session, id-028feeaf,
original direction"
2010-06-09 16:02:28 id=36870 trace_id=22 msg="DNAT 200.202.114.251:80-
>10.123.123.10:80"
2010-06-09 16:02:28 id=36870 trace_id=22 msg="send to ips"
2010-06-09 16:02:28 id=36870 trace_id=23 msg="vd-root received a packet(proto=6,
200.189.190.105:53489->200.202.114.251:80) from wan1."
2010-06-09 16:02:28 id=36870 trace_id=23 msg="Find an existing session, id-028feeaf,
original direction"
2010-06-09 16:02:28 id=36870 trace_id=23 msg="DNAT 200.202.114.251:80-
>10.123.123.10:80"
2010-06-09 16:02:28 id=36870 trace_id=23 msg="send to ips"
2010-06-09 16:02:28 id=36870 trace_id=24 msg="vd-root received a packet(proto=6,
200.189.190.105:53489->200.202.114.251:80) from wan1."
```

```
2010-06-09 16:02:28 id=36870 trace_id=24 msg="Find an existing session, id-028feeaf,
original direction"
2010-06-09 16:02:28 id=36870 trace_id=24 msg="DNAT 200.202.114.251:80-
>10.123.123.10:80"
2010-06-09 16:02:28 id=36870 trace_id=24 msg="send to ips"
2010-06-09 16:02:28 id=36870 trace_id=25 msg="vd-root received a packet(proto=6,
200.189.190.105:53489->200.202.114.251:80) from wan1."
2010-06-09 16:02:28 id=36870 trace_id=25 msg="Find an existing session, id-028feeaf,
original direction"
2010-06-09 16:02:28 id=36870 trace_id=25 msg="DNAT 200.202.114.251:80-
>10.123.123.10:80"
2010-06-09 16:02:28 id=36870 trace_id=25 msg="send to ips"
2010-06-09 16:02:28 id=36870 trace_id=26 msg="vd-root received a packet(proto=6,
200.189.190.105:53490->200.202.114.251:80) from wan1."
2010-06-09 16:02:28 id=36870 trace_id=26 msg="allocate a new session-028feeb0"
2010-06-09 16:02:28 id=36870 trace_id=26 msg="find SNAT: IP-10.123.123.10(from
IPPOOL), port-80"
2010-06-09 16:02:28 id=36870 trace_id=26 msg="VIP-10.123.123.10:80, outdev-wan1"
2010-06-09 16:02:28 id=36870 trace_id=26 msg="DNAT 200.202.114.251:80-
>10.123.123.10:80"
2010-06-09 16:02:28 id=36870 trace_id=26 msg="find a route: gw-10.123.123.10 via
internal"

Fortigate51B # diagnose debug disable
```

21 Command Line Interface (CLI) – Comandos Úteis

21.1 grep

Exemplo 1: mostrar linha de match ignorando diferenças entre maiúsculas e minúsculas (- i)

```
Fortigate51B # get system performance status | grep -i idle
CPU states: 3% user 0% system 0% nice 97% idle
```

Exemplo 2: mostrar 1 linha antes do match (-B 1)

```
FG_RENNER_HA1 # sh full-configuration system interface | grep -B 1 port11
config system interface
    edit "port11"
```

Exemplo 3: mostrar 6 linhas após o match (-A 6)

```
FG_RENNER_HA1 # sh system interface | grep -A 6 port13
    edit "port13"
        set vdom "root"
```

```
        set ip 200.143.61.68 255.255.255.224
        set allowaccess ping
        set type physical
        set description "Antiga porta ETH0 do Brick."
    next
```

21.2 show full-configuration

```
Fortigate51B # show full-configuration
#config-version=FG50BH-4.00-FW-build272-100331:opmode=0:vdom=0
#conf_file_ver=14300459513520570275
#buildno=0272
#global_vdom=1
config system global
    set access-banner disable
    set admin-concurrent enable
    set admin-https-pki-required disable
    set admin-lockout-duration 60
    set admin-lockout-threshold 3
    set admin-maintainer enable
    set admin-port 80
    set admin-scp disable
    set admin-server-cert "self-sign"
    set admin-sport 443
```

21.3 show full-configuration <config block>

Apresentar a configuração completa para apenas uma parte da configuração

```
FG_RENNER_HA1 # sh full-configuration system ha
config system ha
    set group-id 0
    set group-name "FGT-HA"
    set mode a-p
    set password ENC
mtfmBm7ClnEnG579q5NF+OhaOXype9ZgdyjfeyTZb6FLT623xdV3VGkneU2wu6GcPfbcswgKVXv44mYZO0TT
wfNj54M+YCXGnz0k7WpTGj65Yzkd
    set hbdev "port2" 50 "port16" 50
    set route-ttl 10
    set route-wait 0
    set route-hold 10
    set sync-config enable
    set encryption disable
    set authentication disable
    set hb-interval 2
    set hb-lost-threshold 6
    set helo-holddown 20
    set arps 5
```

```
    set arps-interval 8
    set session-pickup enable
    set link-failed-signal disable
    set uninterruptable-upgrade enable
    set ha-mgmt-status disable
    set ha-eth-type "8890"
    set hc-eth-type "8891"
    set l2ep-eth-type "8893"
    set subsecond disable
    set vcluster2 disable
    set override disable
    set priority 128
    set monitor "port2" "port16"
    unset pingserver-monitor-interface
    set pingserver-failover-threshold 0
    set pingserver-flip-timeout 60
end
```

21.4 get system performance status

```
Fortigate51B # get system performance status
CPU states: 0% user 13% system 0% nice 87% idle
Memory states: 33% used
Average network usage: 30720 kbps in 1 minute, 16453 kbps in 10 minutes, 8129 kbps
in 30 minutes
Average sessions: 21 sessions in 1 minute, 19 sessions in 10 minutes, 22 sessions in
30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 0 days,  22 hours,  50 minutes
```

21.5 get system performance top

```
Fortigate51B # get system performance top
Run Time:  16 days, 0 hours and 57 minutes
17U, 4S, 15I; 502T, 130F, 129KF
       ipsengine     3049      S <     1.9    14.8
         miglogd       25      S       1.9     2.5
          newcli      726      R       0.9     2.7
          httpsd       67      S       0.0     6.6
          httpsd       63      S       0.0     6.5
         cmdbsvr       15      S       0.0     4.4
          httpsd       27      S       0.0     3.0
          newcli      707      S       0.0     2.7
          newcli       80      S       0.0     2.6
          newcli     1400      S       0.0     2.6
         sslvpnd       52      S       0.0     2.3
       scanunitd     5867      S <     0.0     2.3
```

```
         updated       54      S       0.0     2.3
  merged_daemons       45      S       0.0     2.2
            iked      444      S       0.0     2.2
       forticron       46      S       0.0     2.2
       urlfilter       48      S       0.0     2.1
        fdsmgmtd       55      S       0.0     2.1
       scanunitd     5845      S <     0.0     2.1
```

21.6 get hardware status

```
Fortigate51B # get hardware status
Model name: Fortigate-51B
ASIC version: CP6
ASIC SRAM: 64M
CPU: Geode(TM) Integrated Processor by AMD PCS
RAM: 502 MB
Compact Flash: 122 MB /dev/hda
Hard disk: 30711 MB /dev/hde
USB Flash: not available
Network Card chipset: ip175c-vdev (rev.)
```

21.7 get system status

```
Fortigate51B # get system status
Version: Fortigate-51B v4.0,build0272,100331 (MR2)
Virus-DB: 11.00067(2009-11-18 19:05)
Extended DB: 11.00067(2009-11-18 19:06)
IPS-DB: 2.00720(2009-12-01 17:55)
FortiClient application signature package: 1.169(2010-04-08 13:02)
Serial-Number: FG50BH3G09600388
BIOS version: 04000005
Log hard disk: Available
Hostname: Fortigate51B
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Distribution: International
Branch point: 272
Release Version Information: MR2
System time: Thu Apr  8 13:19:25 2010
```

21.8 get system interface physical

```
Fortigate51B # get system interface physical
== [onboard]
        ==[internal]
                mode: static
                ip: 10.123.123.1 255.255.255.0
                ipv6: ::/0
                status: up
                speed: 100Mbps (Duplex: full)
        ==[wan1]
                mode: static
                ip: 200.202.114.250 255.255.255.248
                ipv6: ::/0
                status: up
                speed: 100Mbps (Duplex: full)
        ==[wan2]
                mode: static
                ip: 0.0.0.0 0.0.0.0
                ipv6: ::/0
                status: down
                speed: n/a
        ==[modem]
                mode: static
                ip: 0.0.0.0 0.0.0.0
                ipv6: ::/0
                status: down
                speed: n/a
```

21.9 show system interface

```
Firewall1 # sh system interface
config system interface
    edit "port11"
        set vdom "root"
    next
    edit "port12"
        set vdom "root"
    next
    edit "port13"
        set vdom "root"
        set type physical
    next
    edit "port14"
        set vdom "root"
        set type physical
    next
    edit "port15"
        set vdom "root"
        set type physical
    next
```

```
    edit "port16"
        set vdom "root"
        set ip 200.189.190.106 255.255.255.240
        set allowaccess ping https ssh snmp
        set type physical
        set description "Conexão à Internet"
        set alias "INTERNET"
    next
…
```

21.10 diagnose hardware deviceinfo nic <port>

```
Firewall # diagnose hardware deviceinfo nic port2
Description             mvl_sw Ethernet driver1.0
System_Device_Name      port2
CPU_port                10
vlanid                  2
FID                     2
num_ports               1
member                  0x0002
cfg                     1-0x1
Current_HWaddr          00:09:0f:d6:d1:ec
Permanent_HWaddr        00:09:0f:d6:d1:ec
State                   up
Link                    up
Speed                   100
Duplex                  full
Rx_Packets              94
Tx_Packets              76
Rx_Bytes                13724
Tx_Bytes                6526

Firewall1 # diagnose hardware deviceinfo nic port16
Driver Name: NP2
Version: 0.92
Chip Revision: 2
BoardSN: ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
Module Name: 200B-256
DDR Size: 256 MB
Bootstrap ID: 18
PCIX-64bit-@133MHz bus: 02:00.0
Admin: up
MAC: 00:09:0f:d6:d1:ea
Permanent_HWaddr: 00:09:0f:d6:d1:ea
Link: up
Speed: 100Mbps
Duplex: Full
Rx Pkts: 388048729
Tx Pkts: 143567
```

```
Rx Bytes: 2409533440
Tx Bytes: 19298304
MAC3 Rx Errors: 0
MAC3 Rx Dropped: 0
MAC3 Tx Dropped: 0
MAC3 FIFO Overflow: 0
MAC3 IP Error: 0

TAE Entry Used: 0
TSE Entry Used: 0
Host Dropped: 0
Shaper Dropped: 0
EEI0 Dropped: 0
EEI1 Dropped: 0
EEI2 Dropped: 0
EEI3 Dropped: 0
IPSEC QFIFO Dropped: 0
IPSEC DFIFO Dropped: 0
PBA: 123/1019/251
Forwarding Entry Used: 0
Offload IPSEC Antireplay ENC Status: Enable
Offload IPSEC Antireplay DEC Status: Enable
Offload Host IPSEC Traffic: Disable
ses mask: 40077dcb
```

21.11 diagnose ip arp list

```
Firewall1 # diagnose ip arp list
index=10 ifname=root 0.0.0.0 00:00:00:00:00:00 state=00000040 use=1032 confirm=7032
update=1032 ref=1
index=14 ifname=port2 192.168.1.100 state=00000020 use=933 confirm=7333 update=933
ref=1
index=9 ifname=port16 200.189.190.97 00:00:0c:07:ac:7a state=00000002 use=0
confirm=32 update=2980 ref=11
```

21.12 diagnose system kill 9

```
Kill the specified Process ID
```

21.13 diag test auth tacacs+ <server_name> <username> <password>

O server_name deve ser previamente configurado (na web interface: Use -> Remote -> Tacacs+) .

```
Firewall1 # diagnose test authserver tacacs+ BR-TB-ACS1 user1 password1
authenticate user 'user1' on server 'BR-TB-ACS1' succeeded
```

Outros serviços de autenticação podem ser também testados:

```
Firewall1 # diagnose test authserver
cert            test certificate authentication
ldap            test ldap server
ldap-digest     test ldap HA1 password query
ldap-search     search ldap server
radius          test radius server
tacacs+         test TACACS+ server
```

21.14 get router info routing-table details

```
Fortigate51B # get router info routing-table details
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*      0.0.0.0/0 [10/0] via 200.202.114.249, wan1
C       10.123.123.0/24 is directly connected, internal
C       200.202.114.248/29 is directly connected, wan1
```

21.15 get system session status

```
Fortigate51B # get system session status
The total number of sessions for the current VDOM: 9988
```

21.16 get system session list

```
Fortigate51B # get system session list
PROTO   EXPIRE SOURCE           SOURCE-NAT       DESTINATION      DESTINATION-NAT
tcp     3600   10.123.123.10:33297 -                10.123.123.1:22   -
tcp     3494   10.123.123.10:49923 200.202.114.250:60299 91.189.90.40:80   -
tcp     3505   10.123.123.10:49922 200.202.114.250:45962 91.189.90.40:80   -
tcp     77     10.123.123.10:49925 200.202.114.250:58253 91.189.90.40:80   -
tcp     107    10.123.123.10:49924 200.202.114.250:41868 91.189.90.40:80   -
udp     74     10.123.123.10:38240 200.202.114.250:48616 200.198.64.83:53  -
tcp     3598   10.123.123.10:53180 200.202.114.250:61236 74.125.9.35:80    -
tcp     92     10.123.123.10:53177 200.202.114.250:61233 74.125.9.35:80    -
tcp     16     10.123.123.10:53175 200.202.114.250:42815 74.125.9.35:80    -
udp     173    10.123.123.10:39446 200.202.114.250:43678 200.198.64.83:53  -
tcp     3599   10.123.123.10:57657 200.202.114.250:55729 200.236.31.1:80   -
```

```
udp      5       10.123.123.10:33812 200.202.114.250:35996 200.198.64.83:53 -
tcp      112     10.123.123.10:58866 200.202.114.250:48506 74.125.47.100:80 -
udp      85      10.123.123.10:36417 200.202.114.250:52937 200.198.64.83:53 -
udp      85      10.123.123.10:56444 200.202.114.250:31988 200.198.64.83:53 -
udp      4       10.123.123.10:52172 200.202.114.250:58180 200.198.64.83:53 -
tcp      3425    10.123.123.10:35686 200.202.114.250:48110 74.125.47.139:80 -
```

21.17 get system arp

```
Fortigate51B # get system arp
Address           Age(min)    Hardware Addr      Interface
200.202.114.249   0           00:0e:38:e8:14:8c wan1
10.123.123.10     1           00:1e:4f:fd:9b:a6 internal
10.123.123.100    0           08:00:27:50:e2:cd internal
10.123.123.101    0           08:00:27:7b:3b:f1 internal
10.123.123.102    0           08:00:27:d6:67:84 internal
```

21.18 show firewall policy

```
Fortigate51B # show firewall policy
config firewall policy
    edit 7
        set srcintf "internal"
        set dstintf "wan1"
            set srcaddr "ServerLab1"
            set dstaddr "all"
        set action accept
        set schedule "always"
            set service "ANY"
        set logtraffic enable
        set nat enable
    next
    edit 4
        set srcintf "internal"
        set dstintf "wan1"
            set srcaddr "Guest1_Internal"
            set dstaddr "all"
        set action accept
        set central-nat enable
        set schedule "always"
            set service "ANY"
        set logtraffic enable
        set nat enable
    next
    edit 3
        set srcintf "wan1"
        set dstintf "internal"
            set srcaddr "all"
            set dstaddr "UbuntuMaster_Ext_Int"
        set action accept
```

```
        set schedule "always"
            set service "ANY"
        set logtraffic enable
    next
end
```

21.19 show firewall address

```
Fortigate51B # show firewall address
config firewall address
    edit "all"
    next
    edit "SSLVPN_TUNNEL_ADDR1"
        set type iprange
        set end-ip 10.0.0.10
        set start-ip 10.0.0.1
    next
    edit "ServerLab1"
        set subnet 10.123.123.10 255.255.255.255
    next
    edit "Guest1_Internal"
        set subnet 10.123.123.100 255.255.255.255
    next
end
```

21.20 show firewall central-nat

```
Fortigate51B # show firewall central-nat
config firewall central-nat
    edit 1
            set orig-addr "Guest1_Internal"
            set nat-ippool "Guest_External"
        set orig-port 1
        set nat-port 1-65535
    next
end
```

21.21 get firewall service custom/group/predefined

```
Fortigate51B # get firewall service predefined HTTP
name                : HTTP
icmpcode            :
icmptype            :
protocol            : TCP/UDP/SCTP
protocol-number     : 6
sctpport-range      :
tcpport-range       : 80:0-65535
udpport-range       :
```

21.22 execute update-ips

```
Fortigate51B # execute update-ips
```

21.23 get system auto-update status

```
Fortigate51B # get system auto-update status
FDN availability:  available at Wed Jun  9 17:25:26 2010

Push update: disable
Scheduled update: enable
        Update daily:   1:01
Virus definitions update: enable
IPS definitions update: enable
Server override: disable
Push address override: disable
Web proxy tunneling: disable
```

21.24 execute factoryreset

```
Fortigate51B # execute factoryreset
This operation will reset the system to factory default!
Do you want to continue? (y/n)
```

22 Diversos

22.1 Firewall e Reverse Path

Durante os testes verificou-se que o Fortigate possui o mecanismo de Reverse Path habilitado por default. As sessões rejeitadas pelo Reverse Path não foram enviadas para o log.

A atuação do Reverse Path foi validada através do teste de flood com endereço de origem spoofado, no seguinte cenário:

Wan1 = interface conectada ao default gateway;
Wan2.111 = interface conectada ao servidor que gerou o flood;
Internal = servidor web atacado (10.123.123.10).

Comando usado para gerar o flood:

```
root@ServerLab2:~#  hping3 10.123.123.10 --baseport 2025 -k -I vlan1111 --rand-
source -p 80 -i u10000 -S
```

```
Fortigate51B # diagnose debug flow filter clear
Fortigate51B # diagnose debug flow filter daddr 10.123.123.10
Fortigate51B # diagnose debug flow show console enable
show trace messages on console
Fortigate51B # diagnose debug flow trace start 3

2010-06-16 17:22:26 id=36870 trace_id=41 msg="vd-root received a packet(proto=6,
180.5.132.130:2025->10.123.123.10:80) from wan2.111."
2010-06-16 17:22:26 id=36870 trace_id=41 msg="allocate a new session-02bece6b"
2010-06-16 17:22:26 id=36870 trace_id=41 msg="reverse path check fail, drop"
2010-06-16 17:22:26 id=36870 trace_id=42 msg="vd-root received a packet(proto=6,
51.40.63.119:2025->10.123.123.10:80) from wan2.111."
2010-06-16 17:22:26 id=36870 trace_id=42 msg="allocate a new session-02bece6c"
2010-06-16 17:22:26 id=36870 trace_id=42 msg="reverse path check fail, drop"
2010-06-16 17:22:26 id=36870 trace_id=43 msg="vd-root received a packet(proto=6,
16.240.99.141:2025->10.123.123.10:80) from wan2.111."
2010-06-16 17:22:26 id=36870 trace_id=43 msg="allocate a new session-02bece6d"
2010-06-16 17:22:26 id=36870 trace_id=43 msg="reverse path check fail, drop"
2010-06-16 17:22:26 id=36870 trace_id=44 msg="vd-root received a packet(proto=6,
1.255.129.204:2025->10.123.123.10:80) from wan2.111."

Fortigate51B # diagnose debug disable
```

22.2 Encontrar Regras que Usam um Determinado Address ou Address Group

Usar os comandos abaixo para descobrir as regras que usam um determinado host:

```
diag sys checkused firewall.addrgrp:name 'Group-Name'
diag sys checkused firewall.address:name 'Address-Name'
```

Exemplo:

```
Firewall1 # diag sys checkused firewall.address:name RemoteClient
entry used by child table srcaddr:name 'RemoteClient' of table
firewall.policy:policyid '1'
entry used by child table dstaddr:name 'RemoteClient' of table
firewall.policy:policyid '2'
```

22.3 Encontrar Objetos que usam uma determinada interface

Usar:

```
diag sys checkused system.interface:name 'Interface Name'
```

Exemplo:

```
Firewall1 # diag sys checkused system.interface:name switch
entry used by table firewall.address:name 'Internal_Network'
entry used by table firewall.address:name 'RemoteClient'
entry used by table firewall.address:name 'SSLVPN_TUNNEL_ADDR1'
entry used by table firewall.address:name 'all'
entry used by table firewall.policy:policyid '2'
entry used by table firewall.policy:policyid '1'
entry used by table firewall.policy:policyid '2'
```

22.4 Configurar Syslog pela CLI

```
config log syslogd setting
unset override
set status enable
set port 1300
set server 10.20.30.1
set csv enable
set reliable disable
set facility local7
end
```

22.5 Recuperar a password do Admin

1. Make sure you have console access.
2. Reboot the device.
3. At the console login prompt, type “maintainer” as the userid, this should be done within 5-10 seconds.
4. Type in bcpbFGTxxxxxxxxxxxxx as the password where xxxxxxxxxxxxx is the S/N of the Fortigate. Note that the serial number is case sensitive.
5. change the admin password using the commands below:

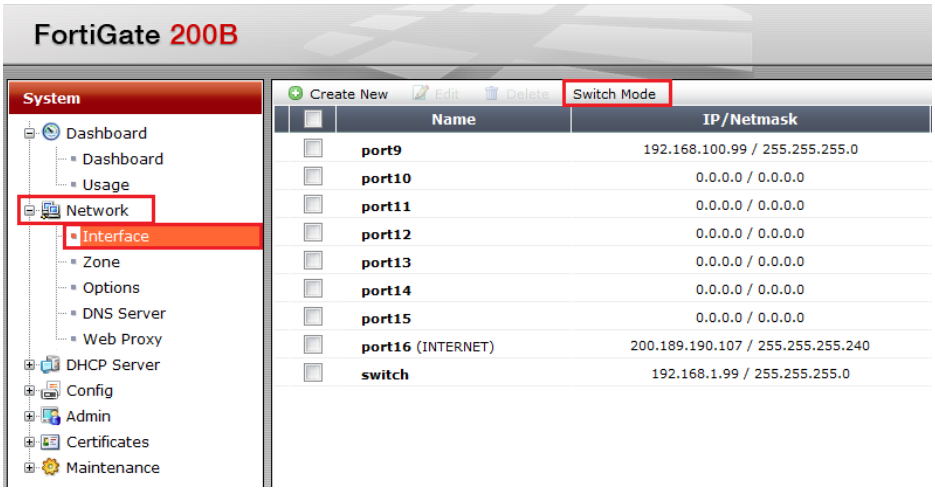
config system admin
edit admin
set password
next
end

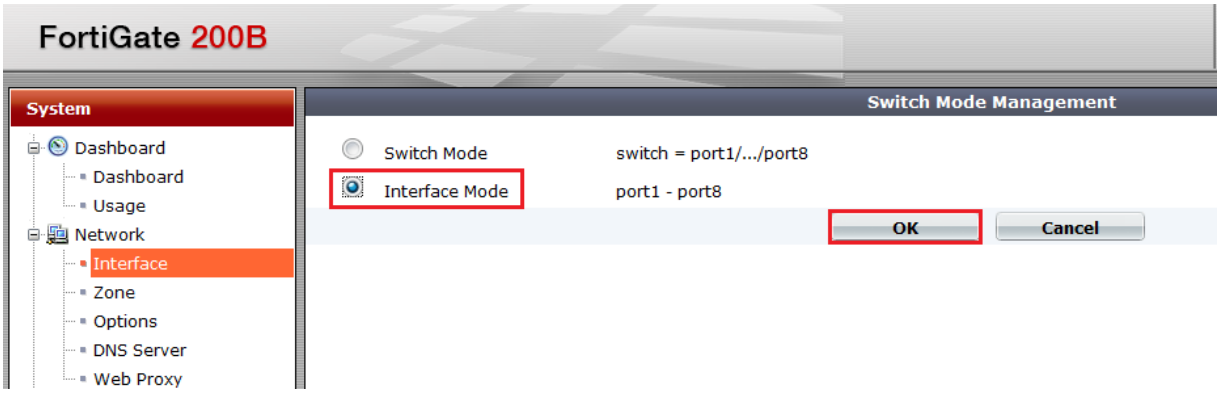
22.6 FortiGate 200B – Converter Interfaces do Switch para Interfaces L3

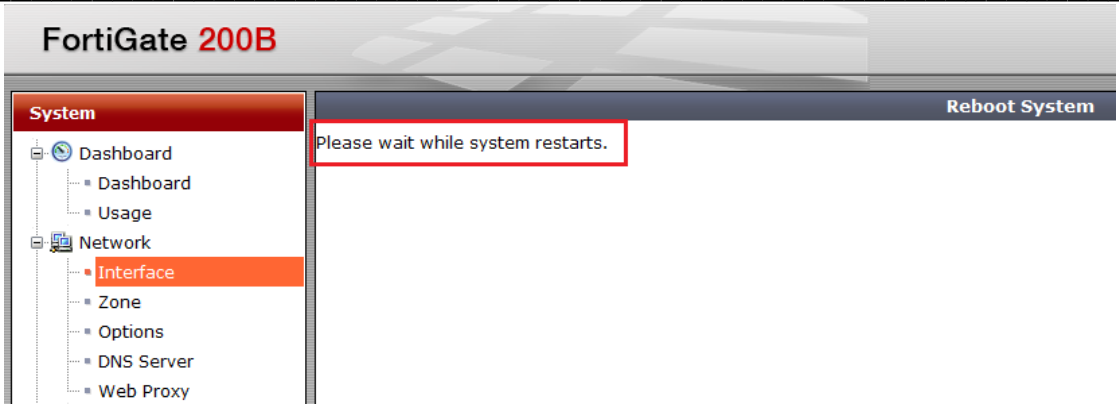
Antes de converter a interface as interfaces de número 1 a 8 para operarem no modo router deve-se apagar as configurações default que fazem referência à interface "switch":

1. Apagar o serviço DHCP existente (System -> DHCP Server -> Service)
2. Apagar a regra default existente (Firewall -> Policy -> Policy)

As telas abaixo apresentam o restante da configuração para converter as interfaces do switch para interfaces de roteamento:







22.7 Creating custom IPS signature to detect

Include this in an IPS sensor as an override. Action "block", "Log" and "quarantine" for, say, 3-10 minutes. For shorter times the list never gets long.

```
F-SBID( --attack_id 2307; --name "SSH.LOGIN.FLOOD.BEDV"; --service SSH; --flow
from_client; --protocol tcp; --tcp_flags S; --rate 2,10; --track src_ip; )
```

--tcp_flags S: catches Syn packets.
--rate 2,10: catches anything above 2 events in 10 seconds.

22.8 Creating custom IPS signature to detect a pattern rate - example to detect a Brute-force attack

Description :Since FortiOS 4.0MR1 and the IPS engine 1.126, there are two new switches available to write custom IPS signatures.

Scope
FortiOS 4.0MR1 and above
IPS engine 1.126 and above.

Solution
Those switches are :

--rate n,t

Triggers if this Signature matches n-times per t-time (seconds). It can be extended using following switch:

--track src_ip || dst_ip

This will extend --rate to further only match "per" source or destination IP. It cannot be used alone but rather is a extension to **--rate**

For example, these can be used to detect an FTP Brute-force where you see multiple "530 Login failed" coming from a Server with a specific IP.

######
F-SBID(--name FTP.Brute.Force; --protocol tcp; --service FTP; --flow from_server; --pattern "530 Login failed"; --rate 5,60; --track src_ip;)
######

This will trigger the Signature only when seeing "--pattern" 5 times per 60 seconds and from the same IP address.

Warning : In that specific case, using the option "Quarantine Attacker" is not a good action, as the Signature that triggers comes from the server IP address and would therefore quarantine the server. Use instead the logging capabilities.

Note : another switch is available, which is "**--flow from_server,reversed;** " ; in this case, even if the signature is triggered "coming from server", the "direction" will be reversed, hence the "Attacker" will be the "Client".
In this situation, only the client will be Quarantined if this action has been set.

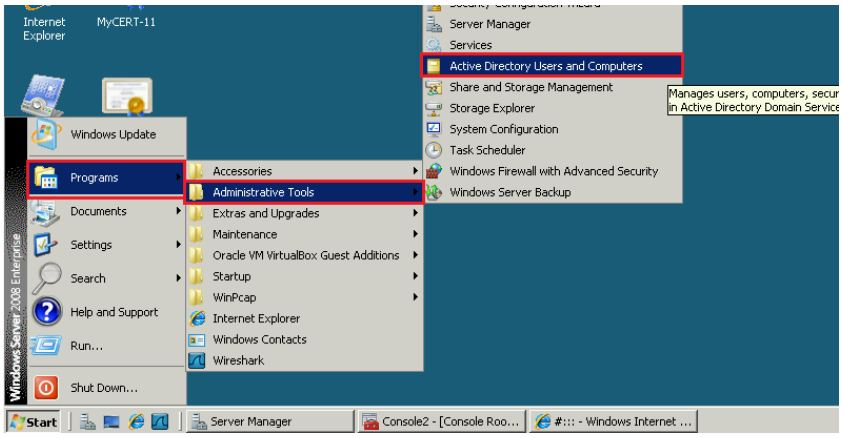
Apêndice I - Autenticação no Windows Active Directory Através de LDAP

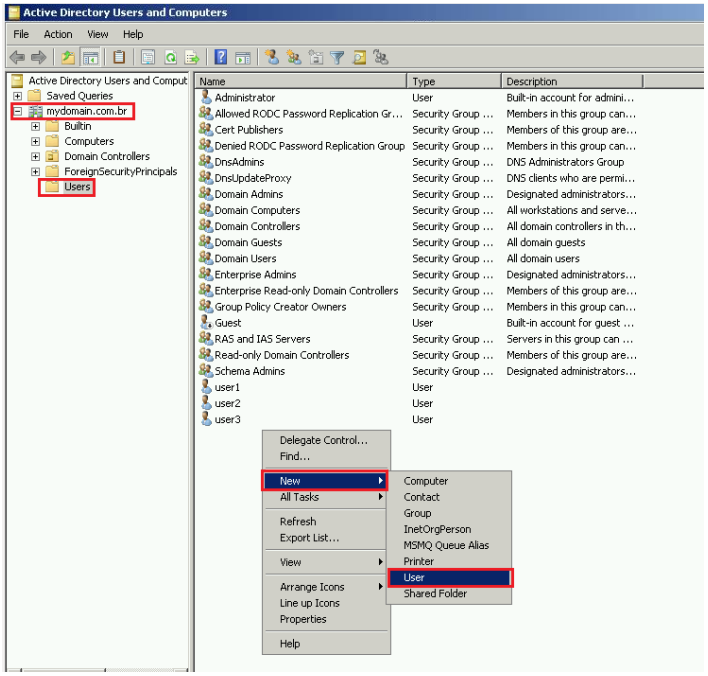
Os processos de autenticação de administradores, VPN SSL e VPN IPSec do FortiGate podem ser integrados ao Windows Active Directory.

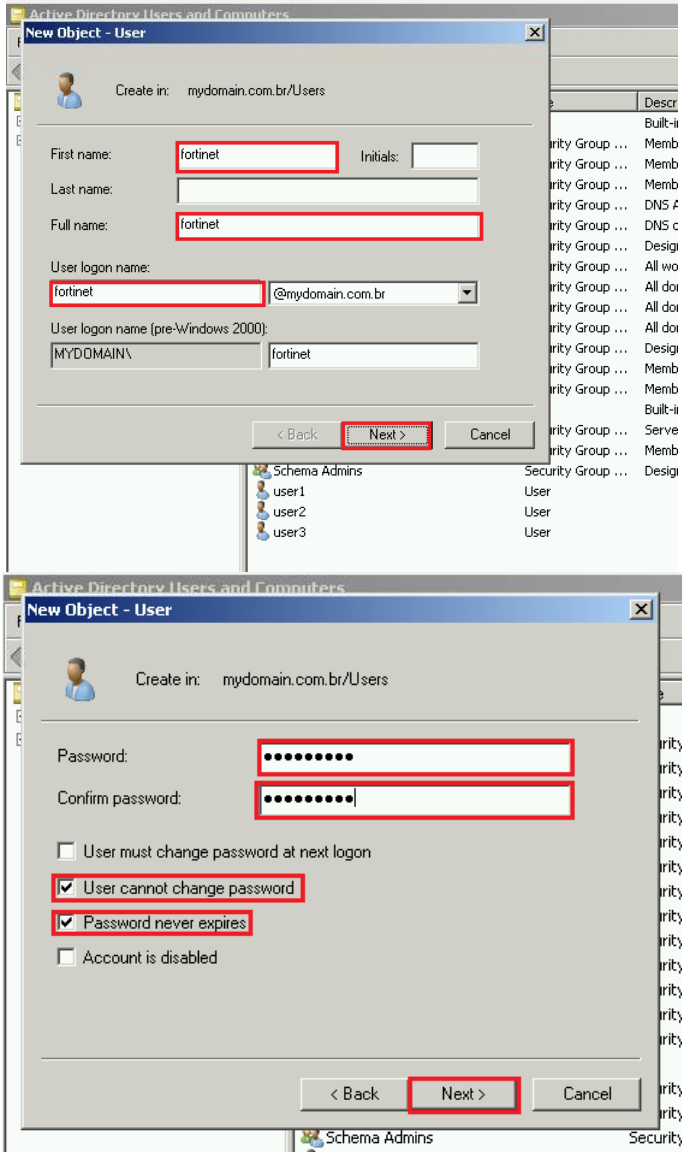
São apresentados a seguir os passos necessários para realizar esta integração usando apenas o protocolo LDAP. Estas configurações são apresentadas apenas a título de exemplo, mas não devem ser implementadas em ambiente de produção devido ao fato de as senhas serem transmitidas entre o FortiGate eo Windows Active Directory sem algum tipo de proteção (criptografia).

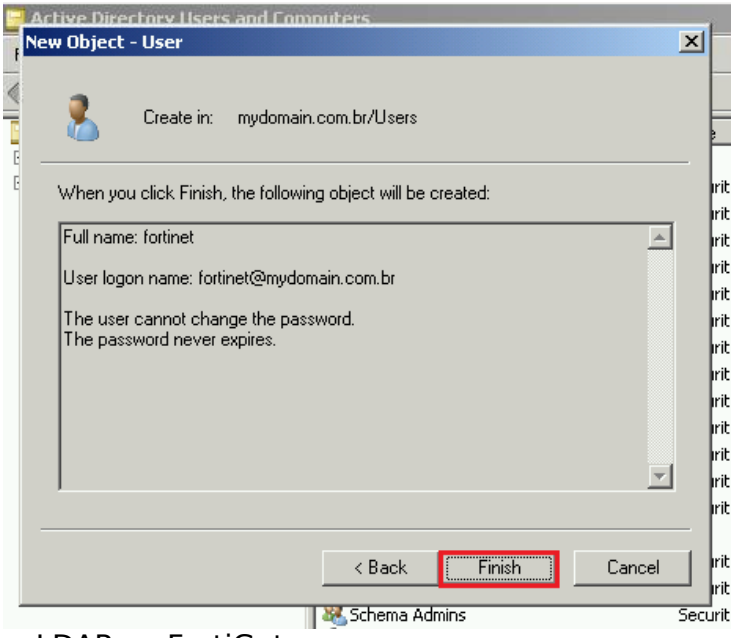
Para ambientes de produção recomenda-se o uso do protocolo LDAPS que implementa a proteção entre o FortiGate e o Windows Active Directory através de SSL. Ver o artigo “Autenticação no Windows Active Directory Através de LDAP over SSL (LDAPS)”.

1. Criar um usuário no Widows Active Directory para fazer as queries.

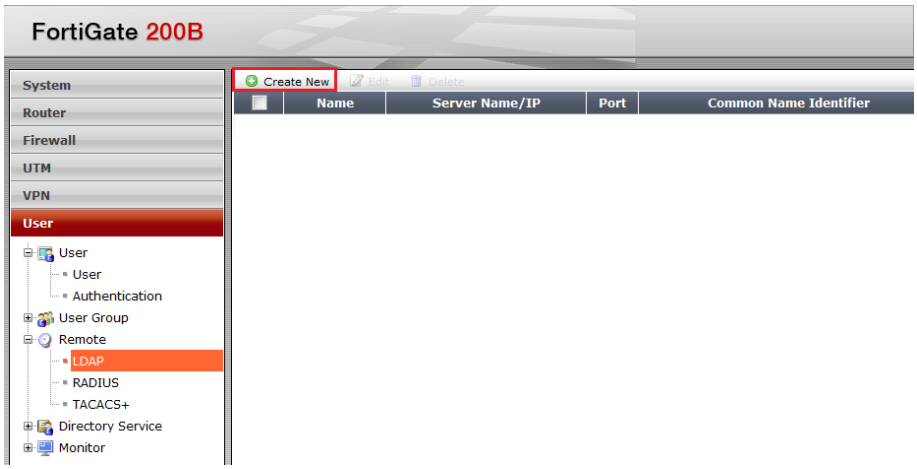





Active Directory Users and Computers
New Object - User
Create in: mydomain.com.br/Users
First name: fortinet
Initials:
Last name:
Full name: fortinet
User logon name:
fortinet
@mydomain.com.br
User logon name (pre-Windows 2000):
MYDOMAIN\
fortinet
< Back
Next >
Cancel
Schema Admins
Security Group ...
user1
User
user2
User
user3
User
Active Directory Users and Computers
New Object - User
Create in: mydomain.com.br/Users
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
< Back
Next >
Cancel
Schema Admins
Security

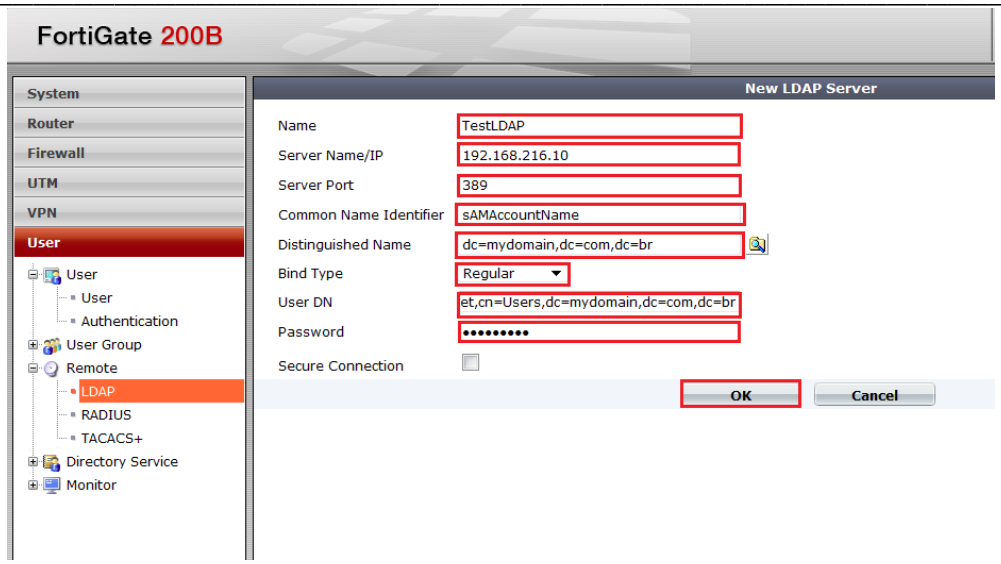


2. Configurar servidor LDAP no FortiGate.



O Distinguished Name define o ponto da árvore de diretórios que será “varrida” através das queries (dc=mydomain,dc=com,dc=br).

O User DN é o Distinguished Name do usuário configurado anteriormente para fazer as queries (Bind). É o usuário anteriormente configurado no Windows Active Directory, e o seu DN é cn=fortinet,cn=Users,dc=mydomain,dc=com,dc=br



3. Realizar testes através da CLI

Habilitar o debug com os comandos:

diagnose debug application fnbamd -1
diagnose debug enable

*Obs: executar o comando **diagnose debug disable** após os testes.

Executar o teste com o comando:

diagnose test authserver ldap <LDAP server> <Windows AD user> <password>

Exemplo de uma autenticação que ocorreu com sucesso:

FG_RENNER_HA1 # **diagnose debug application fnbamd -1**
FG_RENNER_HA1 # **diagnose debug enable**
FG_RENNER_HA1 # **diagnose test authserver ldap TestLDAP user1 Diveo@123**
fnbamd_fsm.c[1010] handle_req-Rcvd auth req 30933001 for user1 in TestLDAP opt=27 prot=0
fnbamd_ldap.c[483] resolve_ldap_FQDN-Resolved address 192.168.216.10, result 192.168.216.10
fnbamd_ldap.c[232] start_search_dn-base:'dc=mydomain,dc=com,dc=br' filter:sAMAccountName=user1
fnbamd_ldap.c[1179] fnbamd_ldap_get_result-Going to SEARCH state
fnbamd_fsm.c[1320] poll_ldap_servers-Continue pending for req 30933001

fnbamd_ldap.c[266] get_all_dn-Found DN
1:CN=user1,CN=Users,DC=mydomain,DC=com,DC=br
fnbamd_ldap.c[280] get_all_dn-Found 1 DN's
fnbamd_ldap.c[314] start_next_dn_bind-Trying DN
1:CN=user1,CN=Users,DC=mydomain,DC=com,DC=br
fnbamd_ldap.c[1217] fnbamd_ldap_get_result-Going to USERBIND state
fnbamd_fsm.c[1320] poll_ldap_servers-Continue pending for req 30933001
fnbamd_ldap.c[372] start_multi_attribute_lookup-Adding attr 'memberOf'
fnbamd_ldap.c[388] start_multi_attribute_lookup-
base:'CN=user1,CN=Users,DC=mydomain,DC=com,DC=br' filter:cn=*

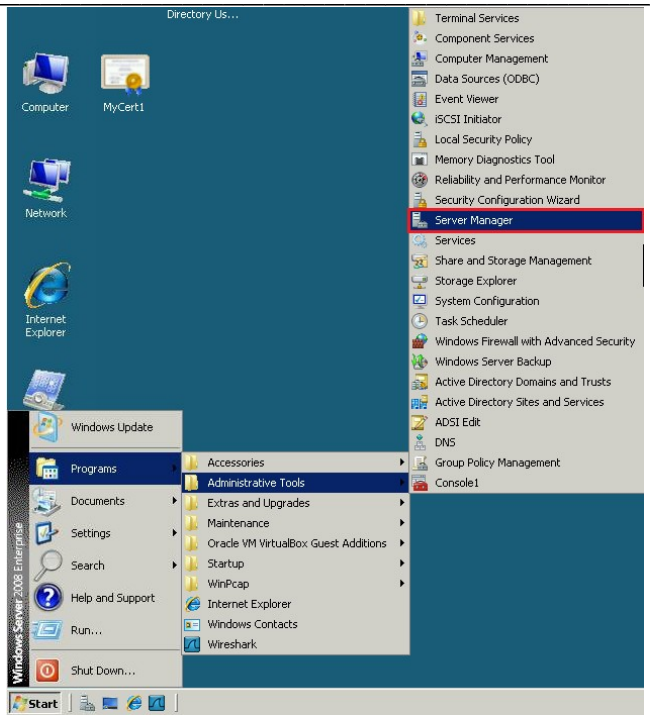
fnbamd_ldap.c[1271] fnbamd_ldap_get_result-Entering CHKUSERATTRS state
fnbamd_fsm.c[1320] poll_ldap_servers-Continue pending for req 30933001
fnbamd_ldap.c[1089] fnbamd_ldap_get_result-Not ready yet
fnbamd_fsm.c[1320] poll_ldap_servers-Continue pending for req 30933001
fnbamd_ldap.c[1089] fnbamd_ldap_get_result-Not ready yet
fnbamd_fsm.c[1320] poll_ldap_servers-Continue pending for req 30933001
fnbamd_ldap.c[1089] fnbamd_ldap_get_result-Not ready yet
fnbamd_fsm.c[1320] poll_ldap_servers-Continue pending for req 30933001
fnbamd_ldap.c[1089] fnbamd_ldap_get_result-Not ready yet
fnbamd_fsm.c[1320] poll_ldap_servers-Continue pending for req 30933001
fnbamd_ldap.c[415] get_member_of_groups-Get the memberOf groups.
fnbamd_ldap.c[434] get_member_of_groups-attr='memberOf' - found 0 values
fnbamd_ldap.c[1285] fnbamd_ldap_get_result-Auth accepted
fnbamd_ldap.c[1300] fnbamd_ldap_get_result-Going to DONE state res=0
fnbamd_auth.c[1543] fnbamd_auth_poll_ldap-Result for ldap svr 192.168.216.10 is SUCCESS
fnbamd_auth.c[1564] fnbamd_auth_poll_ldap-Skipping group matching
fnbamd_comm.c[112] fnbamd_comm_send_result-Sending result 0 for req 30933001
authenticate 'user1' against 'TestLDAP' succeeded!

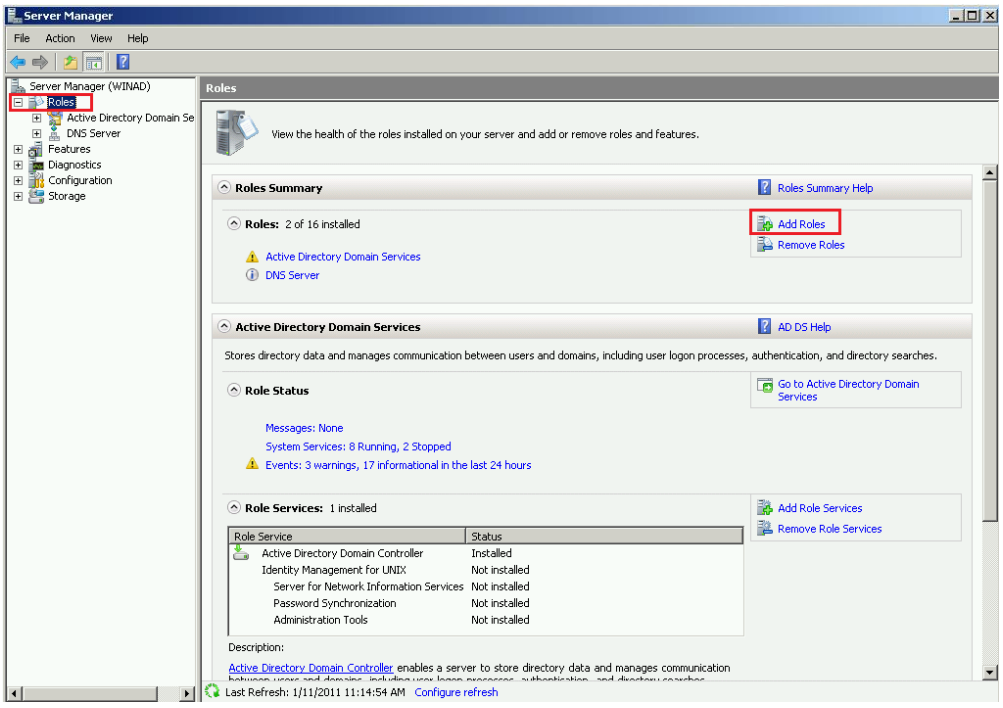
FG_RENNER_HA1 # **diagnose debug disable**

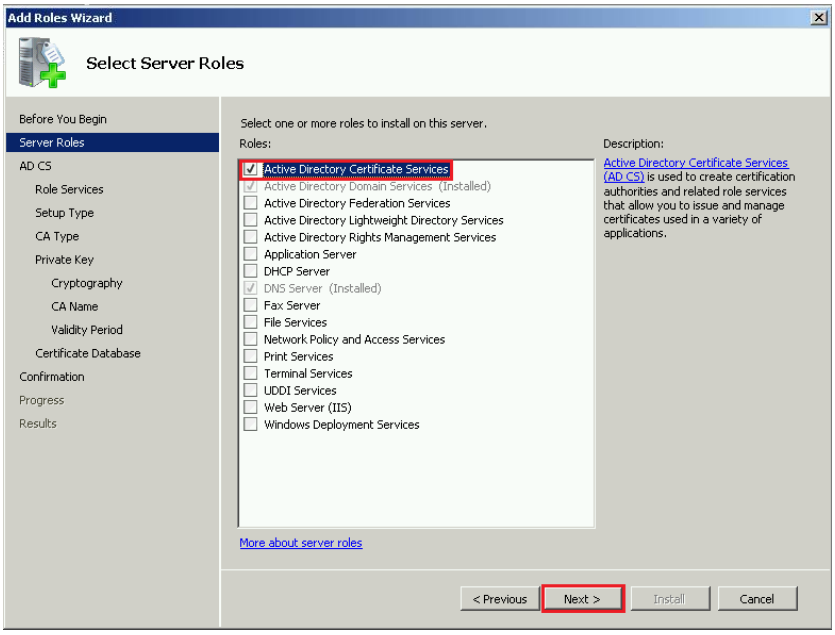
Apêndice II – Autenticação no Windows Active Directory Através de LDAP over SSL (LDAPS)

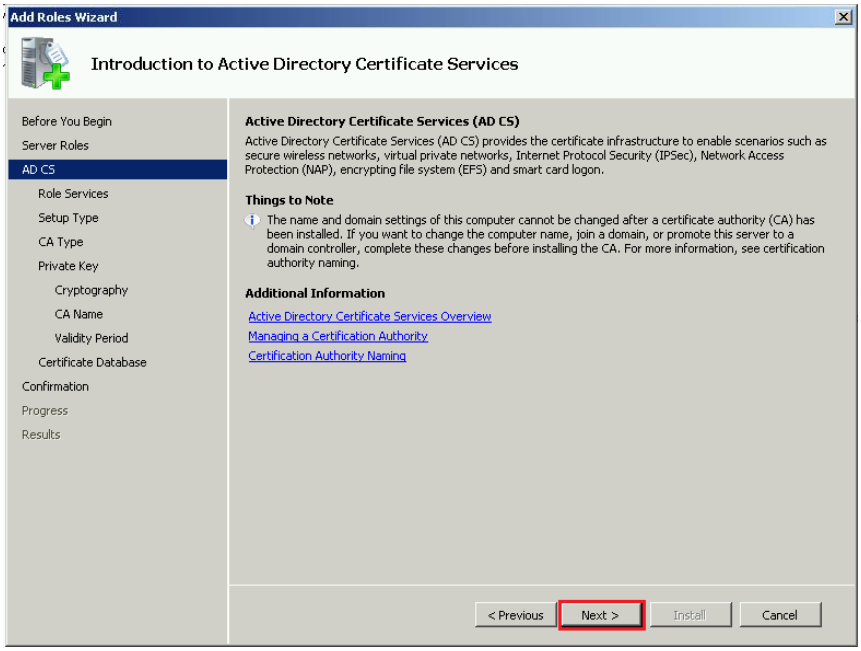
Para que o Windows Active Directory possa responder a queries usando LDAP over SSL é necessário que seja criado um certificado. Os itens 1 e 2 apresentados a seguir mostram como gerar este certificado no Windows 2008.

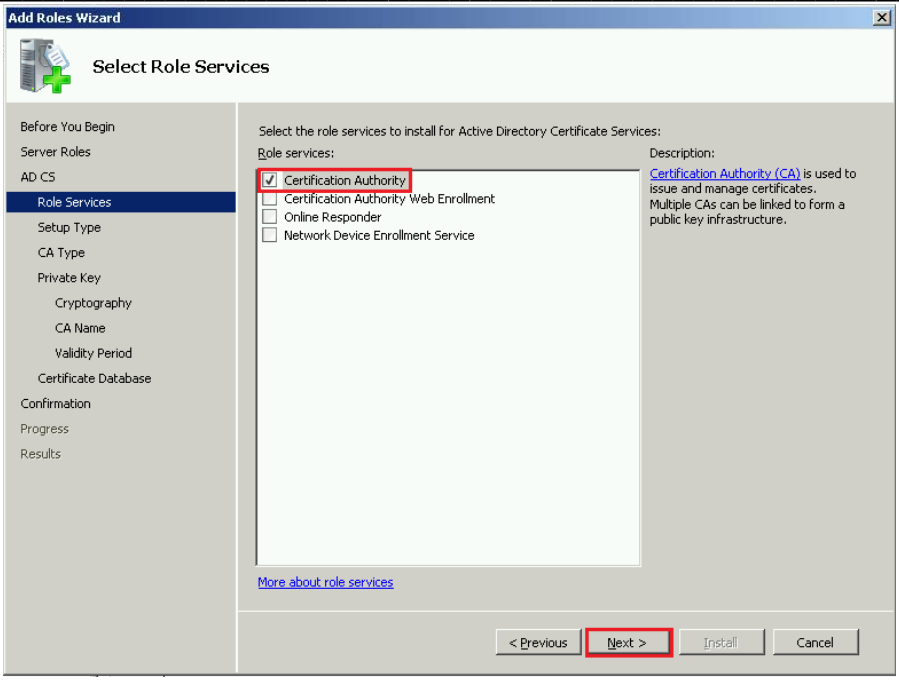
1. Adicionar o Role Active Directory Certificate Services ao servidor Windows 2008 com o Windows Active Directory.

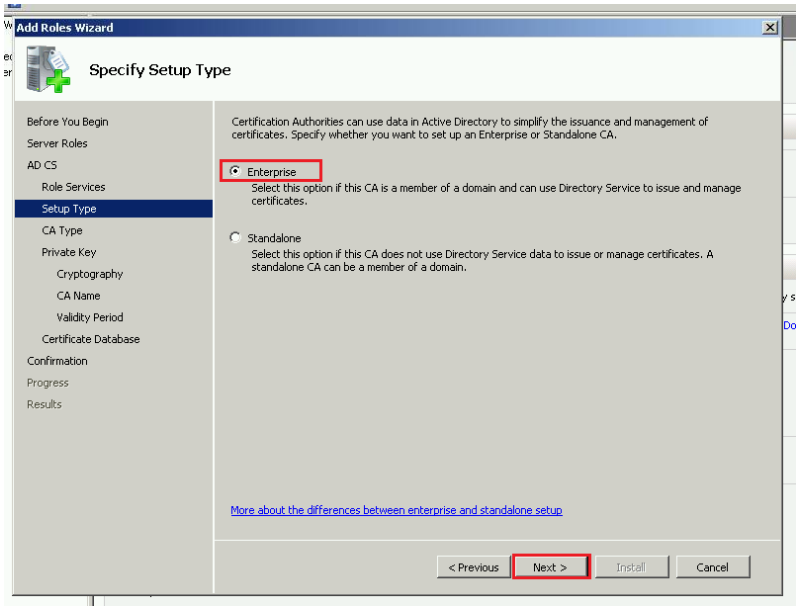

Directory Us...
Computer
MyCert1
Network
Internet Explorer
Windows Update
Programs
Documents
Settings
Search
Help and Support
Run...
Shut Down...
Start
Accessories
Administrative Tools
Extras and Upgrades
Maintenance
Oracle VM VirtualBox Guest Additions
Startup
WinPcap
Internet Explorer
Windows Contacts
Wireshark
Terminal Services
Component Services
Computer Management
Data Sources (ODBC)
Event Viewer
iSCSI Initiator
Local Security Policy
Memory Diagnostics Tool
Reliability and Performance Monitor
Security Configuration Wizard
Server Manager
Services
Share and Storage Management
Storage Explorer
System Configuration
Task Scheduler
Windows Firewall with Advanced Security
Windows Server Backup
Active Directory Domains and Trusts
Active Directory Sites and Services
ADSI Edit
DNS
Group Policy Management
Console1

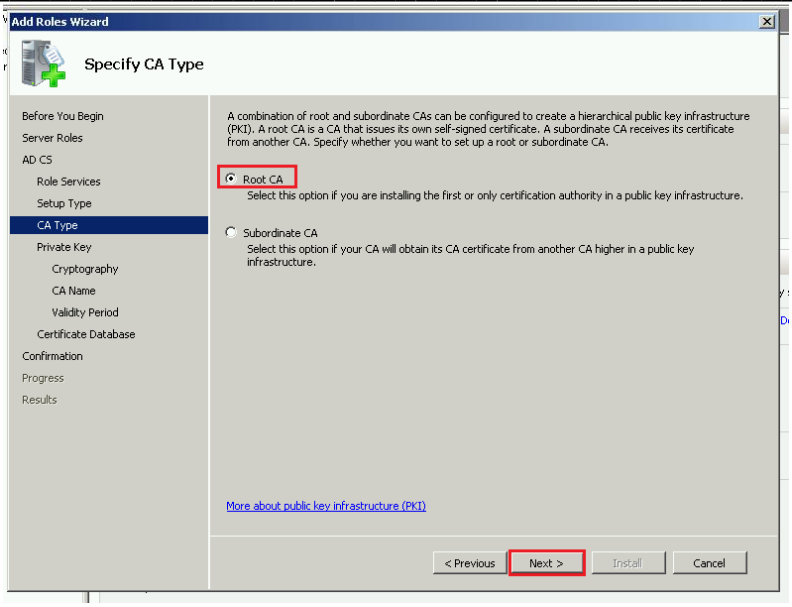

Server Manager
File Action View Help
Server Manager (WINAD)
Roles
Active Directory Domain Se
DNS Server
Features
Diagnostics
Configuration
Storage
Roles
View the health of the roles installed on your server and add or remove roles and features.
Roles Summary
Roles Summary Help
Roles: 2 of 16 installed
Add Roles
Remove Roles
Active Directory Domain Services
DNS Server
Active Directory Domain Services
AD DS Help
Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.
Role Status
Go to Active Directory Domain Services
Messages: None
System Services: 8 Running, 2 Stopped
Events: 3 warnings, 17 informational in the last 24 hours
Role Services: 1 installed
Add Role Services
Remove Role Services
Role Service
Status
Active Directory Domain Controller
Installed
Identity Management for UNIX
Not installed
Server for Network Information Services
Not installed
Password Synchronization
Not installed
Administration Tools
Not installed
Description:
Active Directory Domain Controller enables a server to store directory data and manages communication
Last Refresh: 1/11/2011 11:14:54 AM
Configure refresh

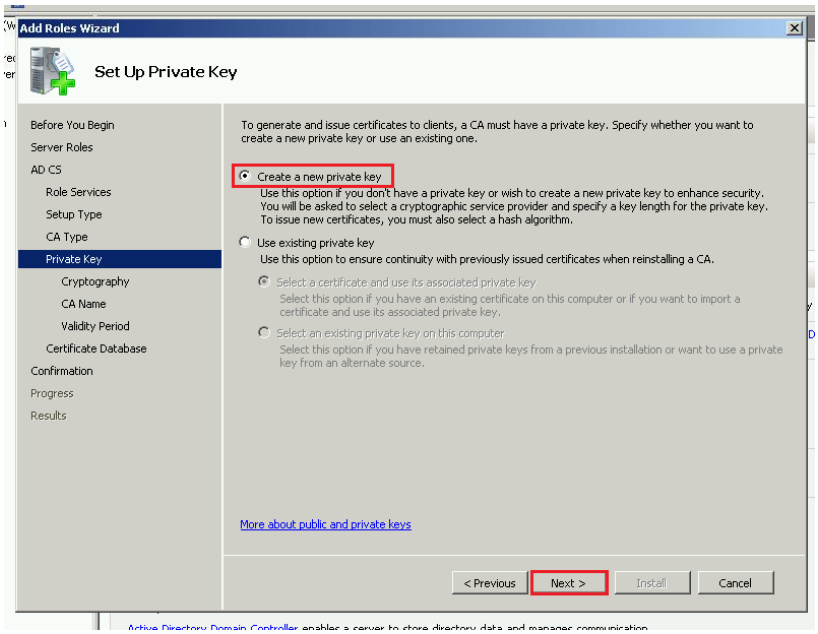

Add Roles Wizard
Select Server Roles
Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Select one or more roles to install on this server.
Roles:
Active Directory Certificate Services
Active Directory Domain Services (Installed)
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Application Server
DHCP Server
DNS Server (Installed)
Fax Server
File Services
Network Policy and Access Services
Print Services
Terminal Services
UDDI Services
Web Server (IIS)
Windows Deployment Services
Description:
Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
More about server roles
< Previous
Next >
Install
Cancel

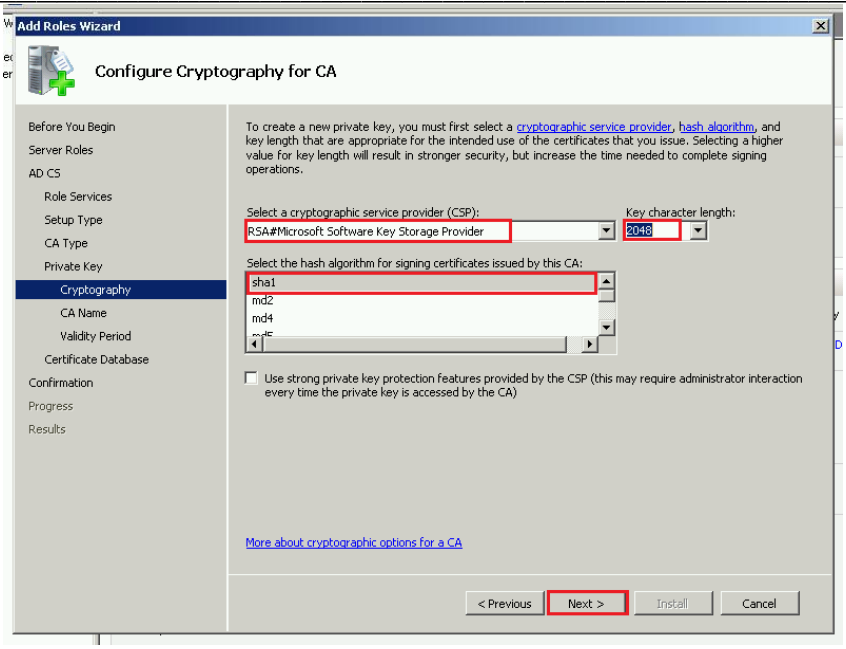

Add Roles Wizard
Introduction to Active Directory Certificate Services
Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Active Directory Certificate Services (AD CS)
Active Directory Certificate Services (AD CS) provides the certificate infrastructure to enable scenarios such as secure wireless networks, virtual private networks, Internet Protocol Security (IPSec), Network Access Protection (NAP), encrypting file system (EFS) and smart card logon.
Things to Note
The name and domain settings of this computer cannot be changed after a certificate authority (CA) has been installed. If you want to change the computer name, join a domain, or promote this server to a domain controller, complete these changes before installing the CA. For more information, see certification authority naming.
Additional Information
Active Directory Certificate Services Overview
Managing a Certification Authority
Certification Authority Naming
< Previous
Next >
Install
Cancel


Add Roles Wizard
Select Role Services
Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Select the role services to install for Active Directory Certificate Services:
Role services:
Certification Authority
Certification Authority Web Enrollment
Online Responder
Network Device Enrollment Service
Description:
Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.
More about role services
< Previous
Next >
Install
Cancel

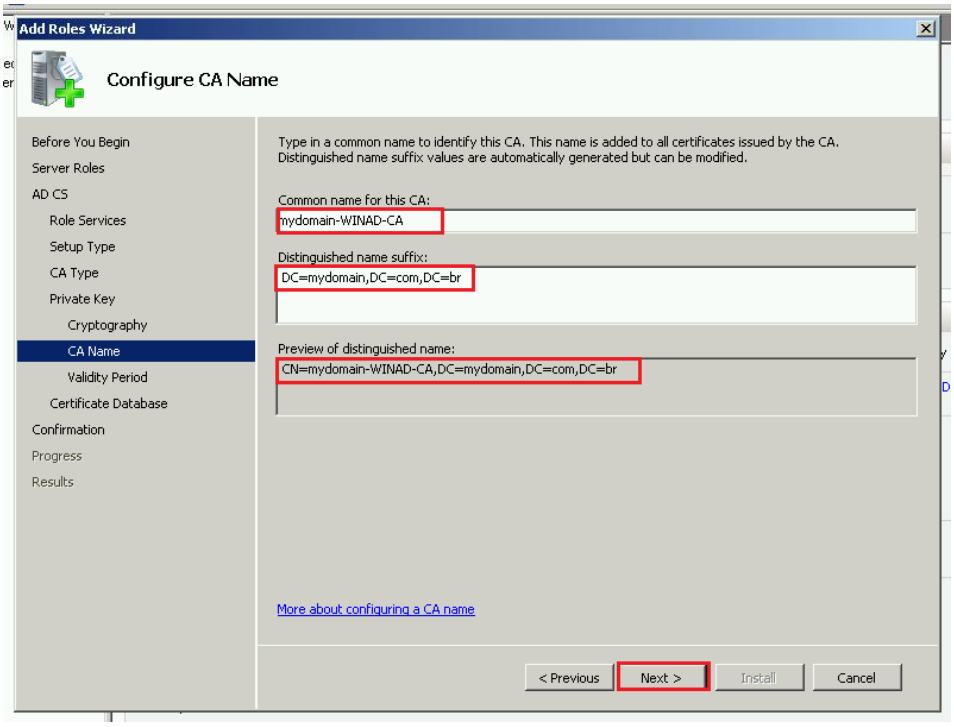

Add Roles Wizard
Specify Setup Type
Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.
Enterprise
Select this option if this CA is a member of a domain and can use Directory Service to issue and manage certificates.
Standalone
Select this option if this CA does not use Directory Service data to issue or manage certificates. A standalone CA can be a member of a domain.
More about the differences between enterprise and standalone setup
< Previous
Next >
Install
Cancel


Add Roles Wizard
Specify CA Type
Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA.
Root CA
Select this option if you are installing the first or only certification authority in a public key infrastructure.
Subordinate CA
Select this option if your CA will obtain its CA certificate from another CA higher in a public key infrastructure.
More about public key infrastructure (PKI)
< Previous
Next >
Install
Cancel

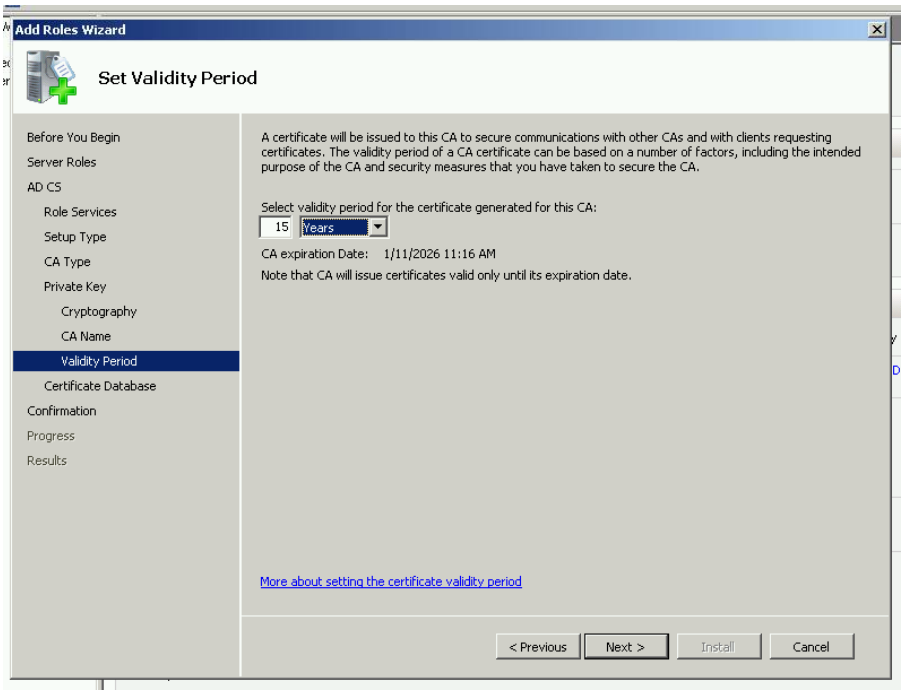

Add Roles Wizard
Set Up Private Key
Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
To generate and issue certificates to clients, a CA must have a private key. Specify whether you want to create a new private key or use an existing one.
Create a new private key
Use this option if you don't have a private key or wish to create a new private key to enhance security. You will be asked to select a cryptographic service provider and specify a key length for the private key. To issue new certificates, you must also select a hash algorithm.
Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.
Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.
Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.
More about public and private keys
< Previous
Next >
Install
Cancel

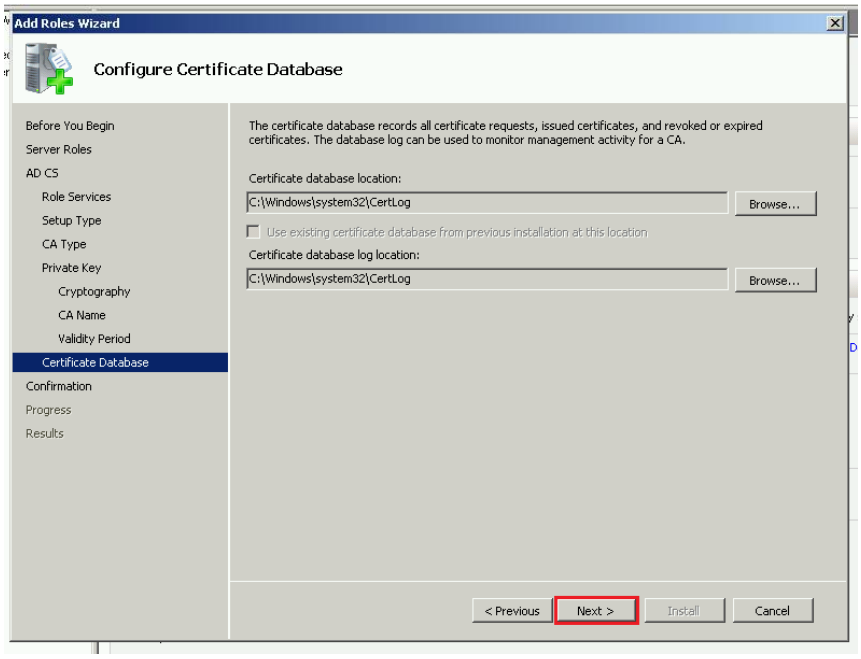


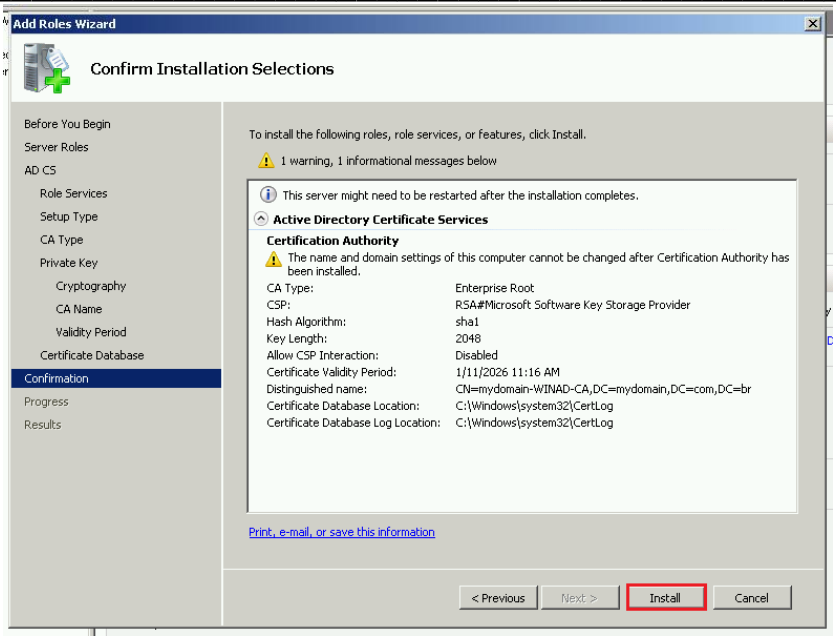
- Aceitar as opções default para o nome da CA.

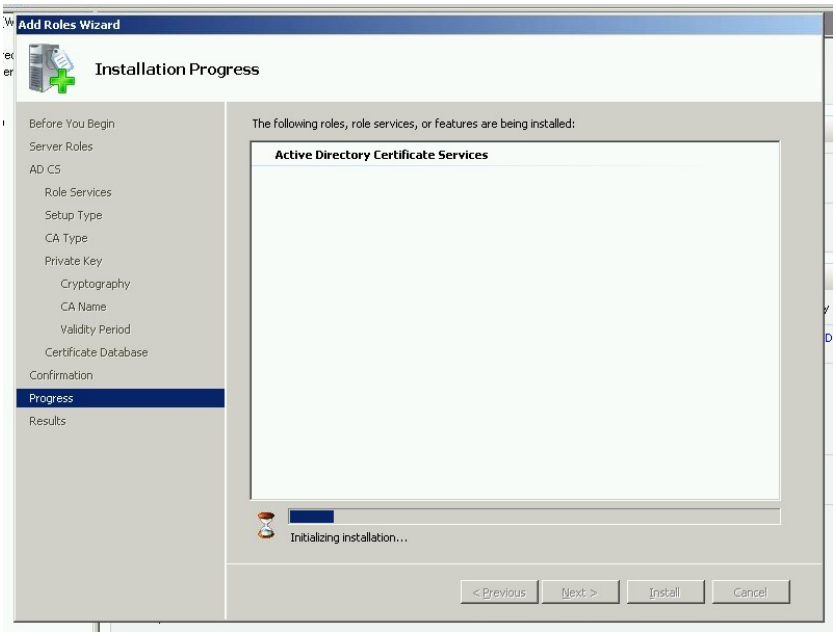


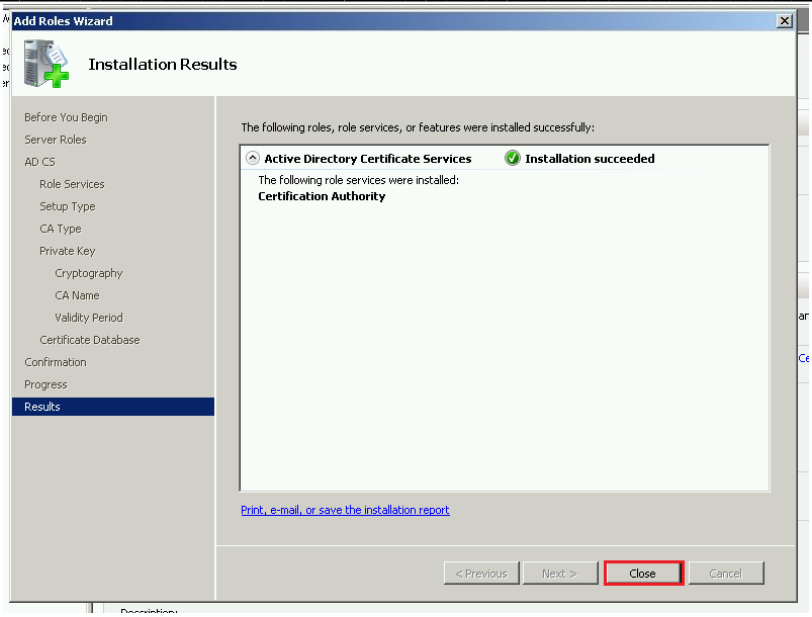
- Ajustar o período de validade do certificado da CA.



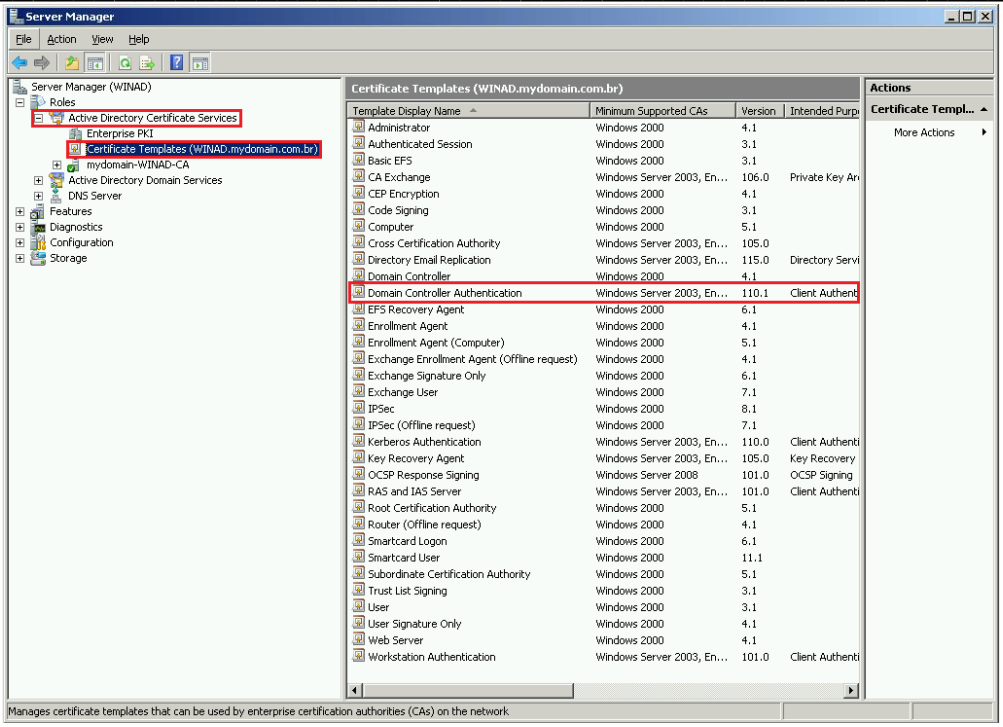



Add Roles Wizard
Confirm Installation Selections
Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
To install the following roles, role services, or features, click Install.
1 warning, 1 informational messages below
This server might need to be restarted after the installation completes.
Active Directory Certificate Services
Certification Authority
The name and domain settings of this computer cannot be changed after Certification Authority has been installed.
CA Type: Enterprise Root
CSP: RSA#Microsoft Software Key Storage Provider
Hash Algorithm: sha1
Key Length: 2048
Allow CSP Interaction: Disabled
Certificate Validity Period: 1/11/2026 11:16 AM
Distinguished name: CN=mydomain-WINAD-CA,DC=mydomain,DC=com,DC=br
Certificate Database Location: C:\Windows\system32\CertLog
Certificate Database Log Location: C:\Windows\system32\CertLog
Print, e-mail, or save this information
< Previous
Next >
Install
Cancel

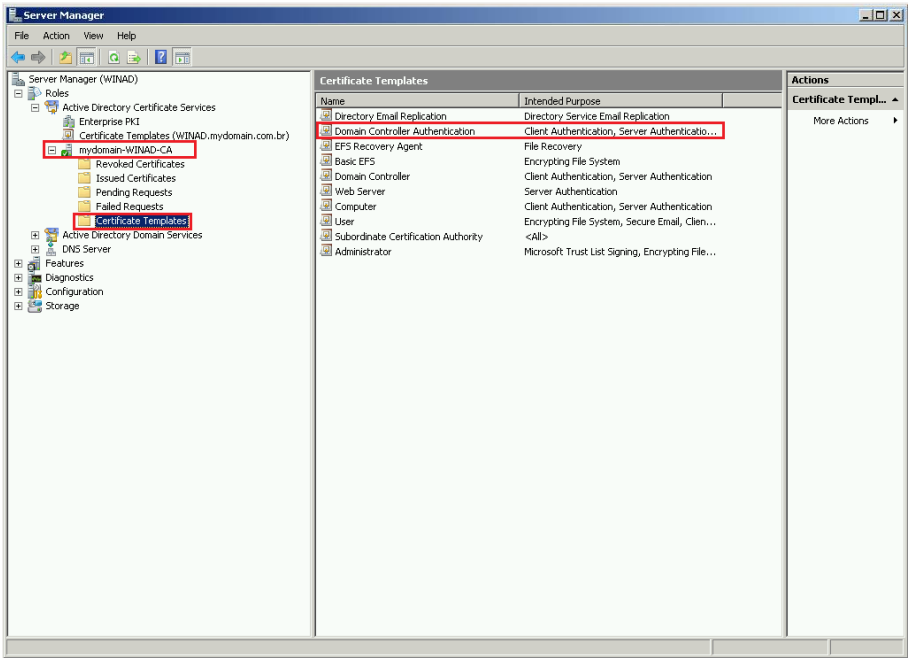

Add Roles Wizard
Installation Progress
Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
The following roles, role services, or features are being installed:
Active Directory Certificate Services
Initializing installation...
< Previous
Next >
Install
Cancel



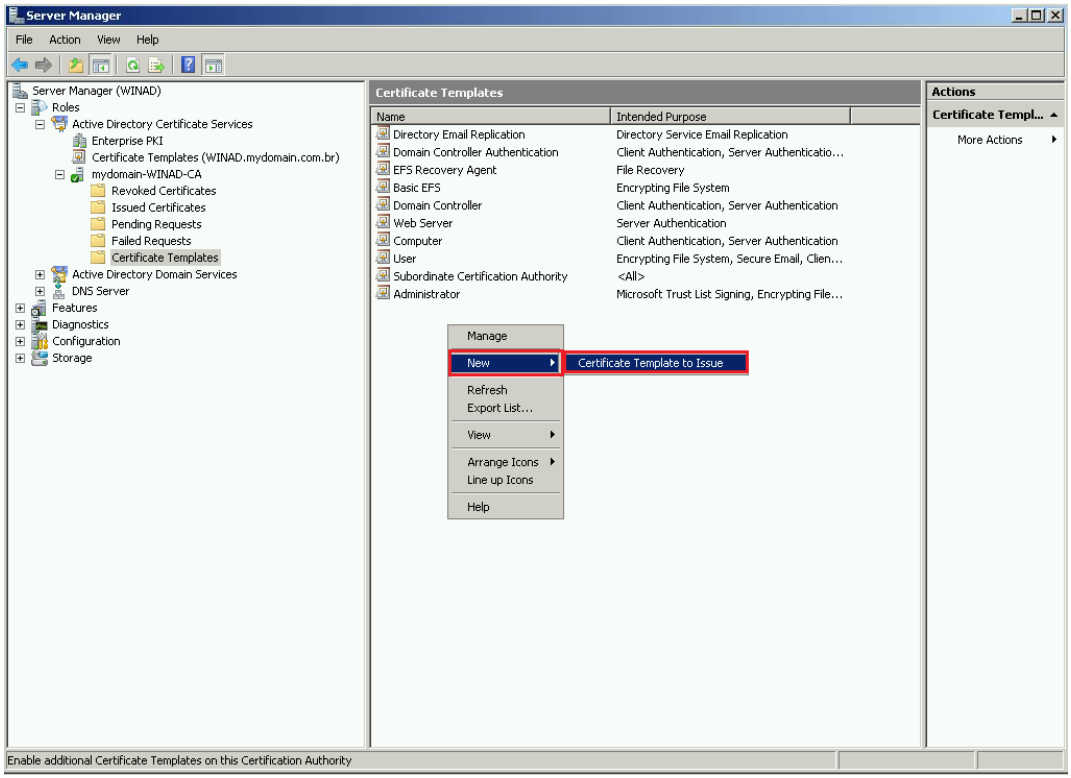
2. Criar o certificado. A criação do certificado será realizada através de templates.
   - Através da console do “Server Manager” navegar até o folder “Certificate Templates”.
   - Verificar se existe o template “Domain Controller Authentication”.



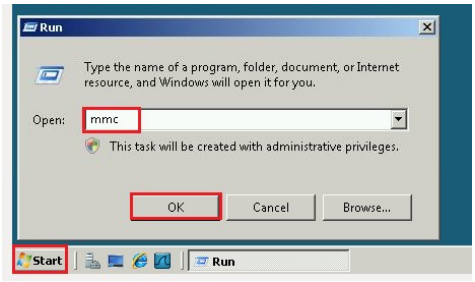
- Verificar se o template “Domain Controller Authentication” também existe no diretório “Certificate Templates” do servidor CA em questão (mydomain-WINAD-CA no exemplo).

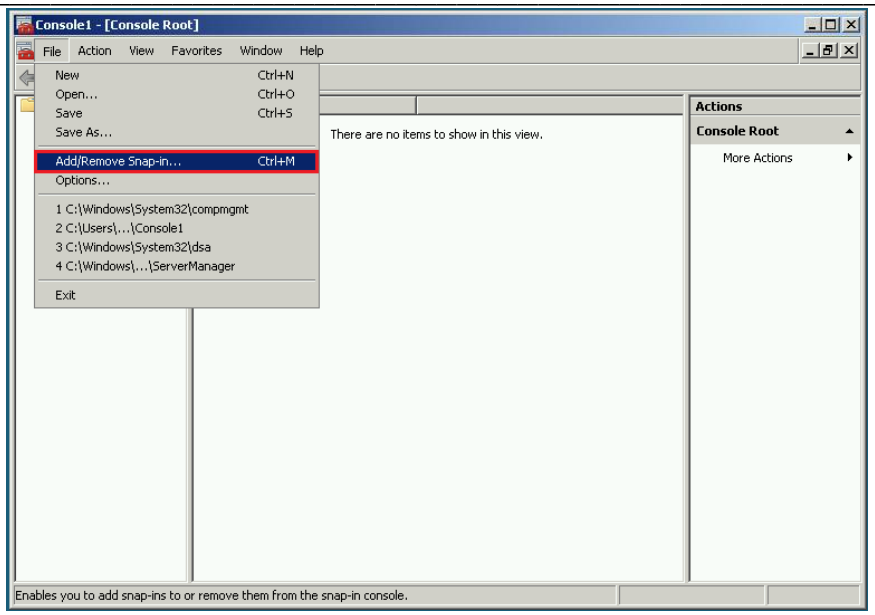


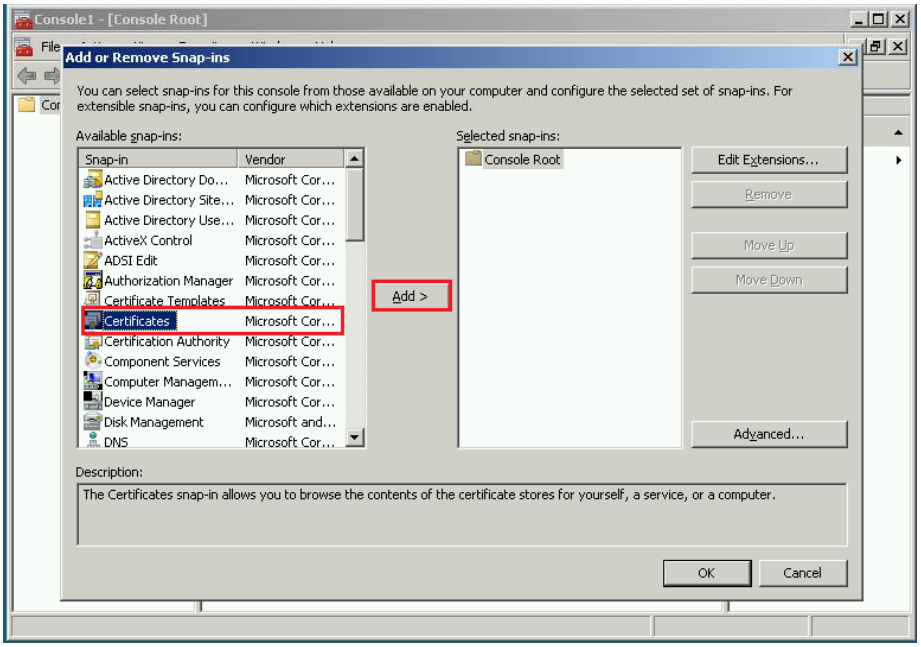
- “Caso” este template não exista no dieretório “Certificate Templates” do servidor CA, ele deve ser adicionado:

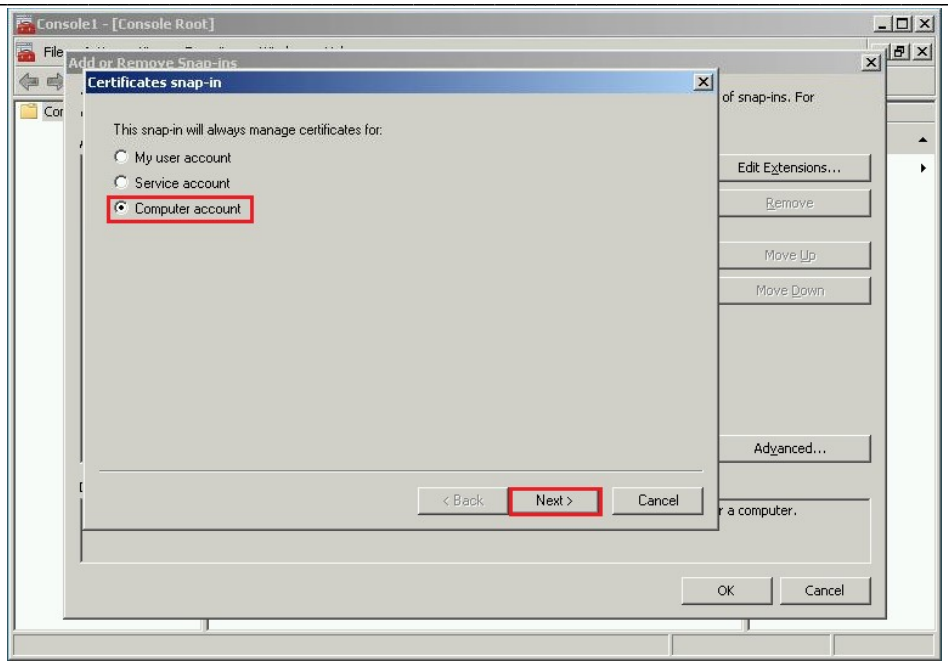


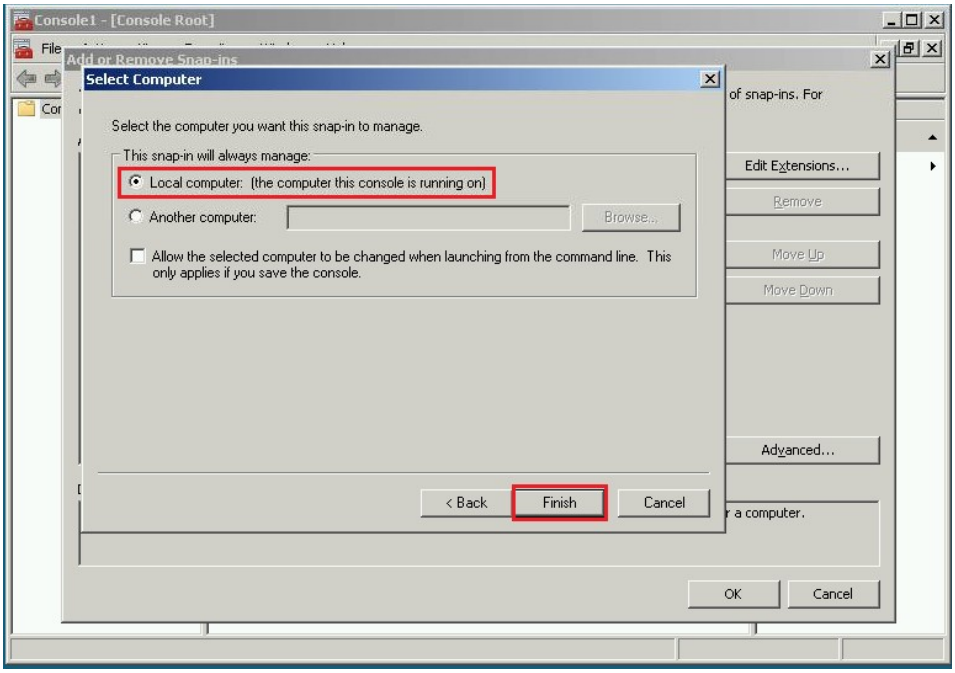
- Gerar um certificado com a ajuda do Snap-in “Certificates” no Microsoft Management Console (MMC).
- Instalar o Snap-in “Certificates” no Microsoft Management Console (MMC)

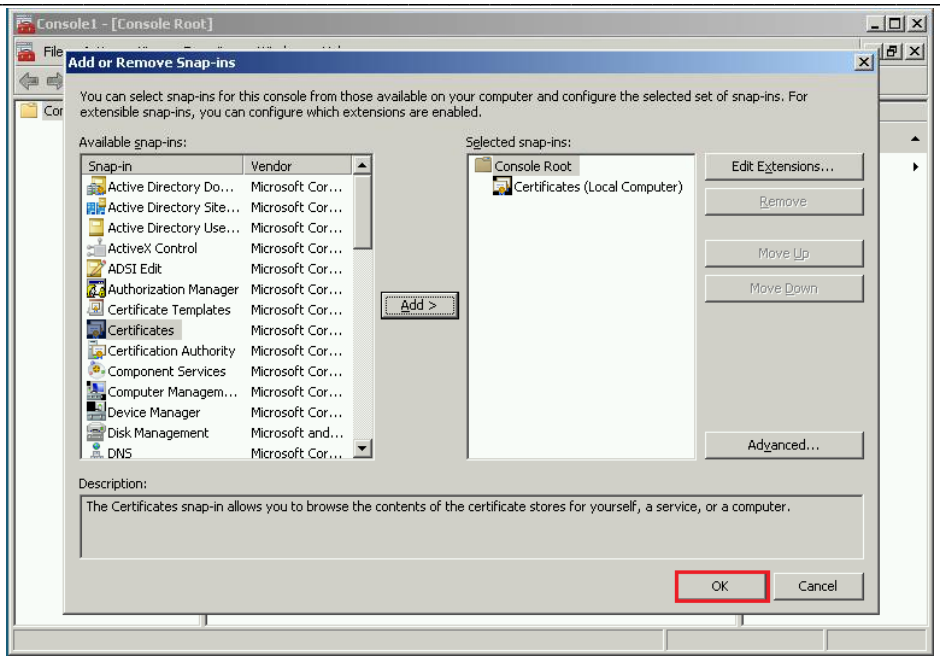



Console1 - [Console Root]
File Action View Favorites Window Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Windows\System32\compmgmt
2 C:\Users\...\Console1
3 C:\Windows\System32\dsa
4 C:\Windows\...\ServerManager
Exit
There are no items to show in this view.
Actions
Console Root
More Actions
Enables you to add snap-ins to or remove them from the snap-in console.

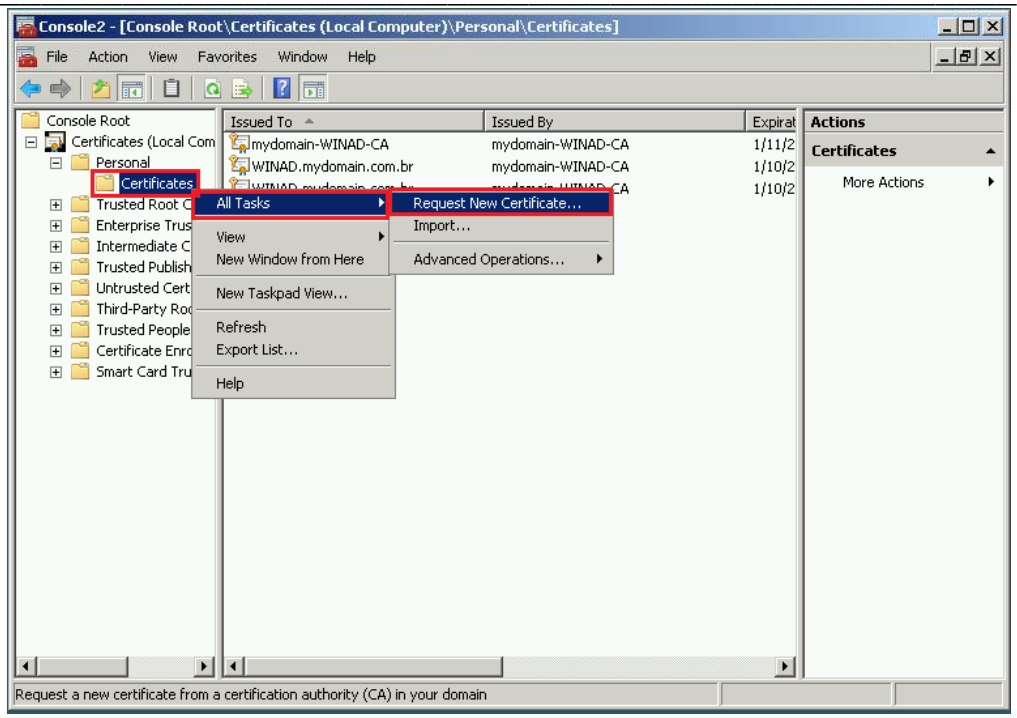

Console1 - [Console Root]
Add or Remove Snap-ins
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.
Available snap-ins:
Snap-in
Vendor
Active Directory Do... Microsoft Cor...
Active Directory Site... Microsoft Cor...
Active Directory Use... Microsoft Cor...
ActiveX Control Microsoft Cor...
ADSI Edit Microsoft Cor...
Authorization Manager Microsoft Cor...
Certificate Templates Microsoft Cor...
Certificates Microsoft Cor...
Certification Authority Microsoft Cor...
Component Services Microsoft Cor...
Computer Managem... Microsoft Cor...
Device Manager Microsoft Cor...
Disk Management Microsoft and...
DNS Microsoft Cor...
Add >
Selected snap-ins:
Console Root
Edit Extensions...
Remove
Move Up
Move Down
Advanced...
Description:
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.
OK
Cancel

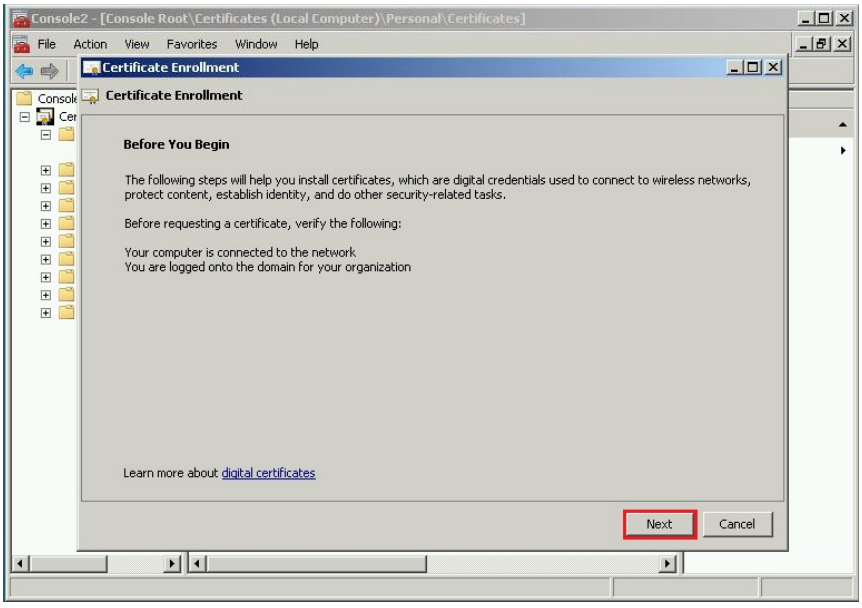

Console1 - [Console Root]
File
Add or Remove Snap-ins
Certificates snap-in
This snap-in will always manage certificates for:
My user account
Service account
Computer account
< Back
Next >
Cancel
of snap-ins. For
Edit Extensions...
Remove
Move Up
Move Down
Advanced...
a computer.
OK
Cancel


Console1 - [Console Root]
File
Add or Remove Snap-ins
Select Computer
Select the computer you want this snap-in to manage.
This snap-in will always manage:
Local computer: (the computer this console is running on)
Another computer:
Browse...
Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.
< Back
Finish
Cancel
of snap-ins. For
Edit Extensions...
Remove
Move Up
Move Down
Advanced...
a computer.
OK
Cancel

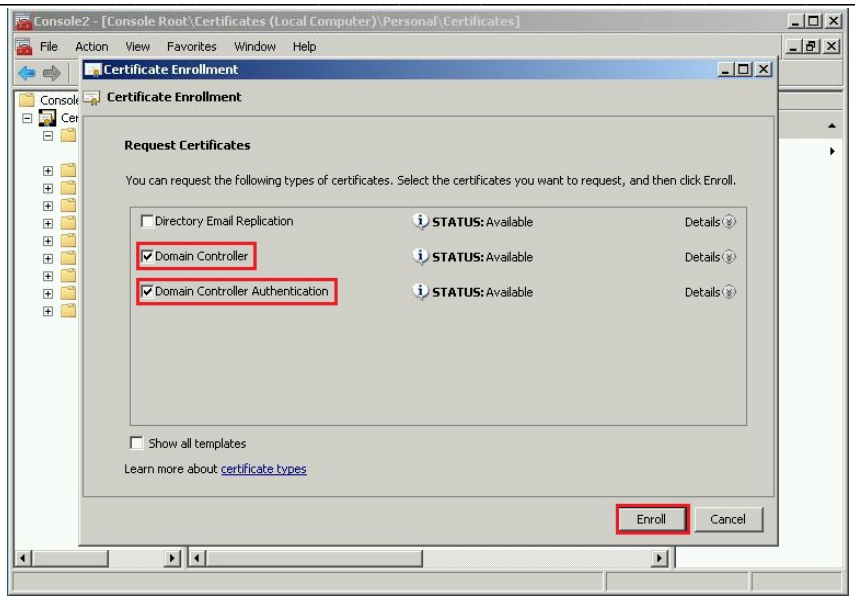


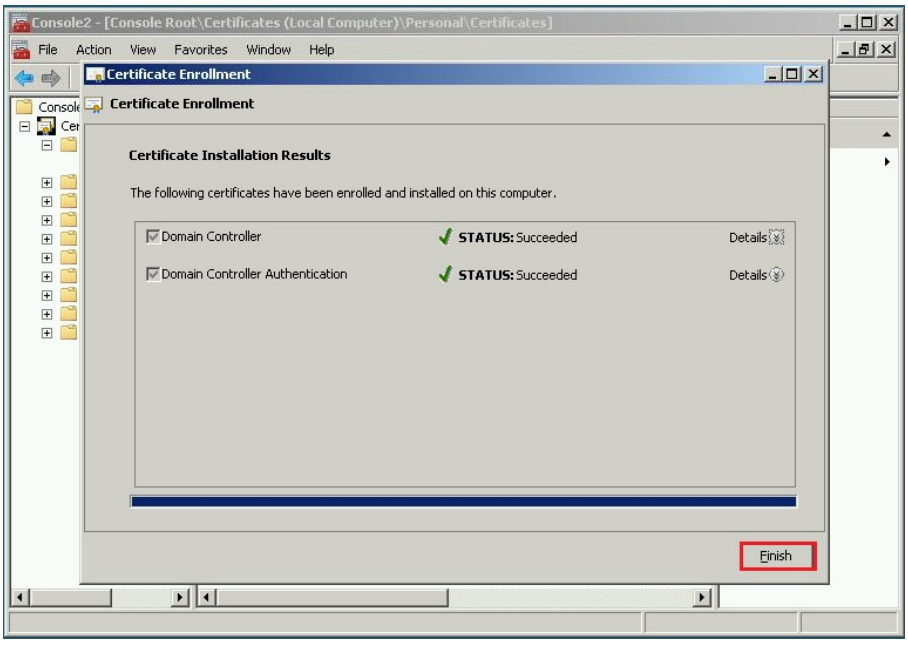
- Gerar o certificado.
- Expandir os folders Certificates -> Personal -> Certificates.
- Clicar com o botão direito sobre Certificates. Selecionar All Tasks e Request Certificate...



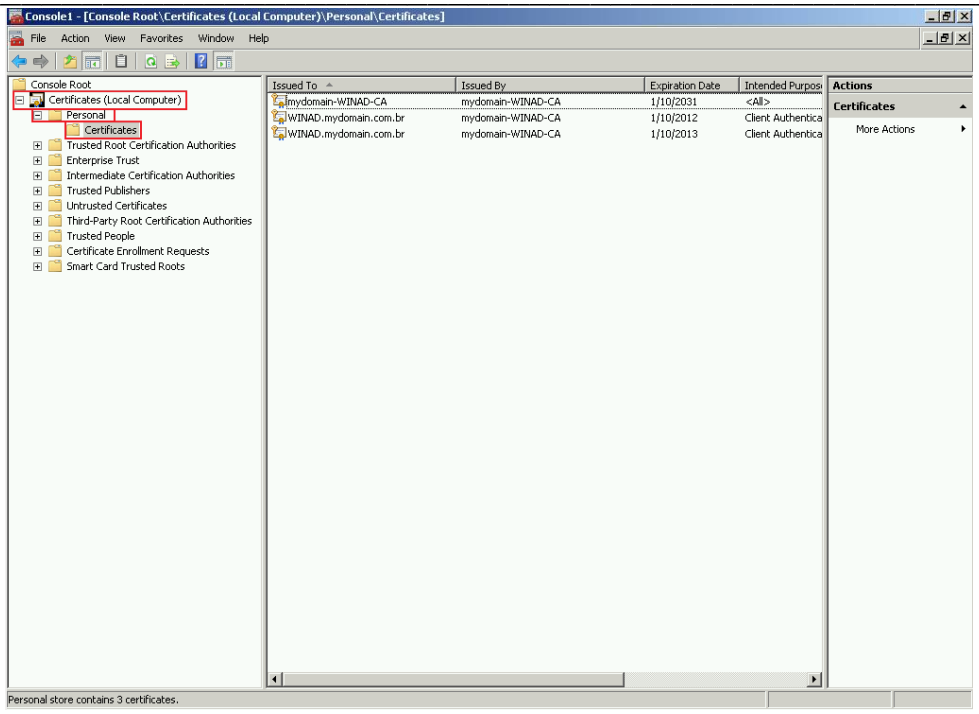


- Selecionar os certificados Domain Controller e Domain Controller Authentication.

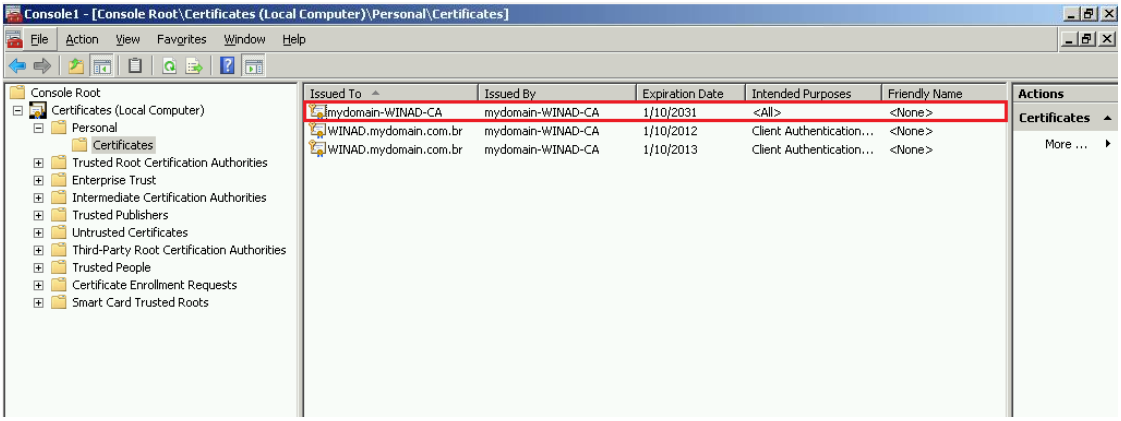




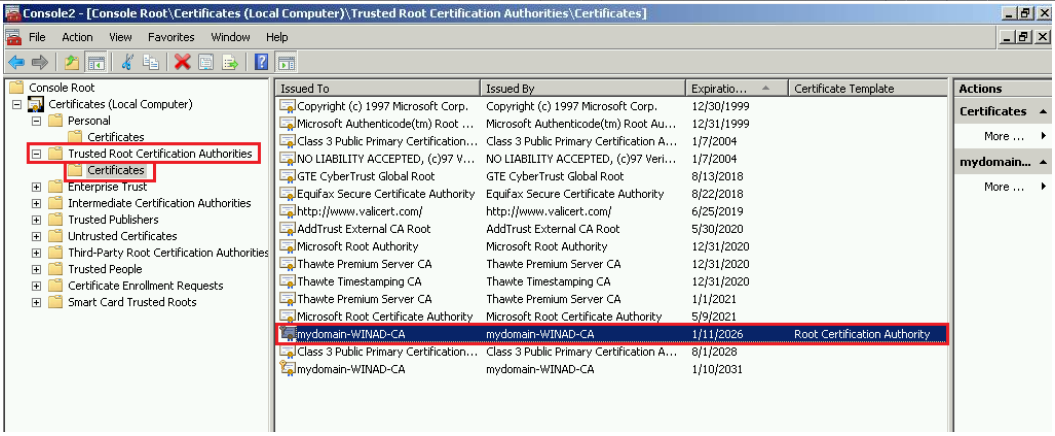
3. Exportar o certificado no Windows AD (com o uso do MMC) e importá-lo no FortiGate.



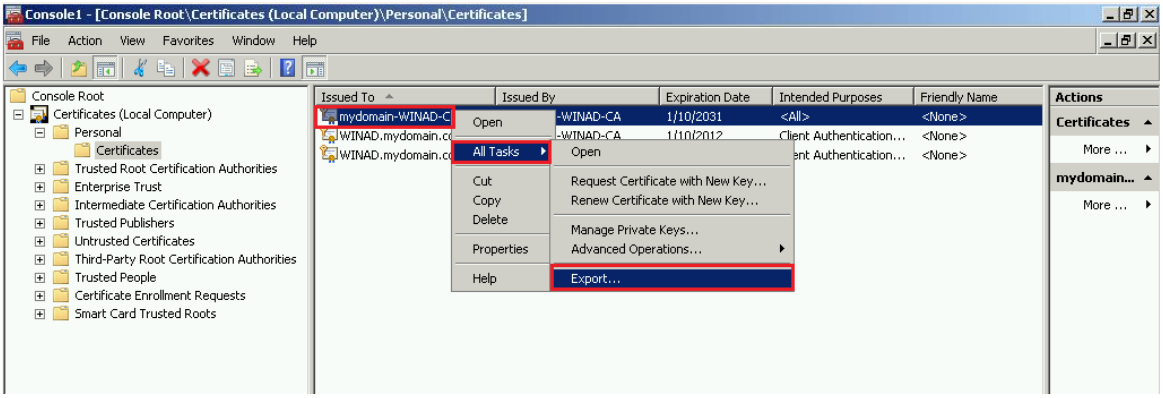
- Selecionar o certificado da Root Certification Authority (no exemplo mydomain-WINAD-CA).

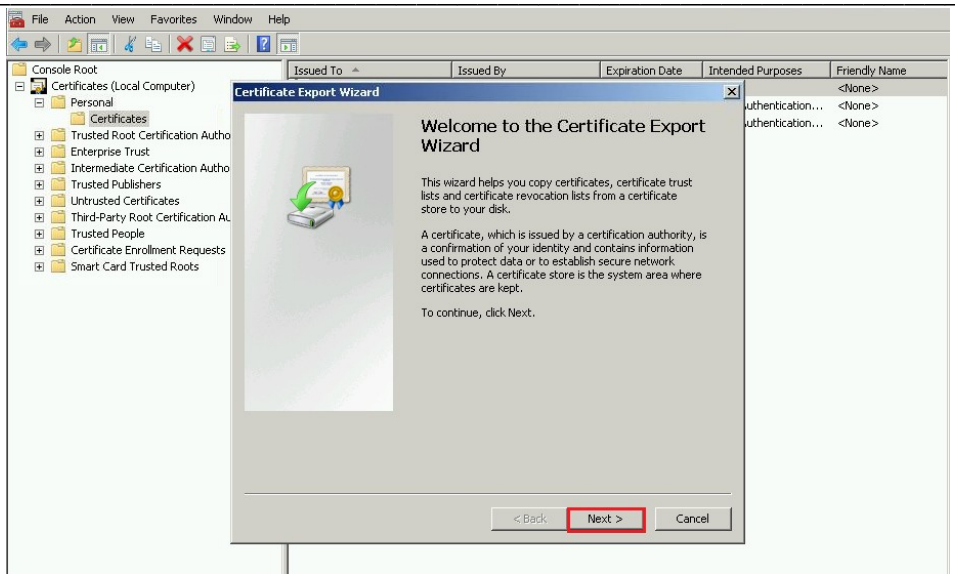


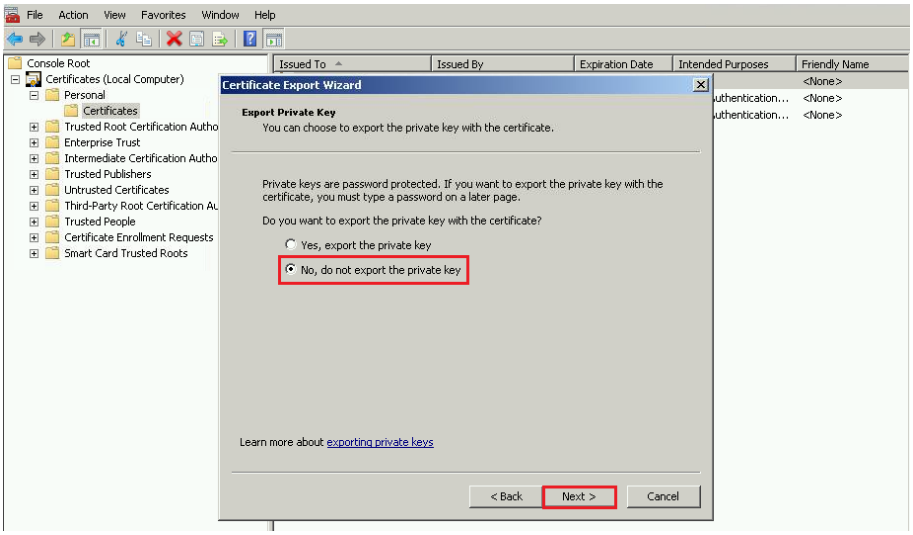
Obs: o certificado da Root Certification Authority também pode ser encontrado na pasta Trusted Root Certification Authority -> Certificates

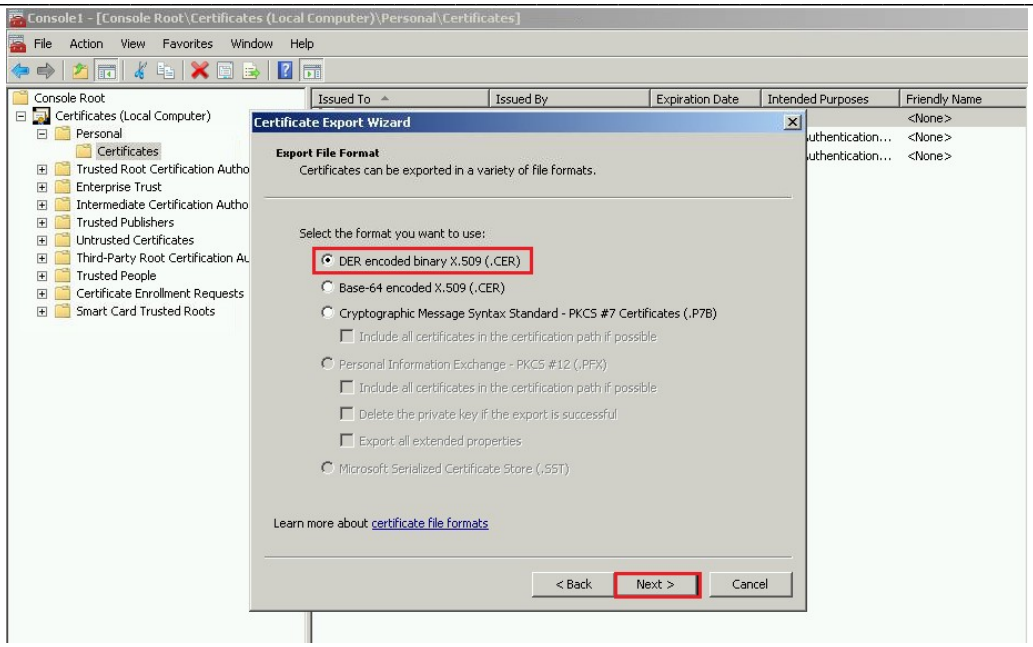


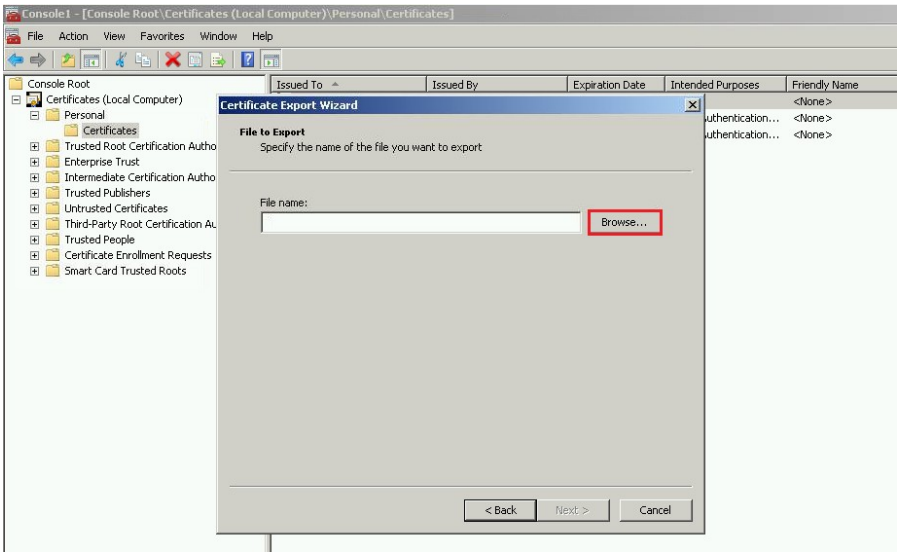
- Executar o export do certificado.

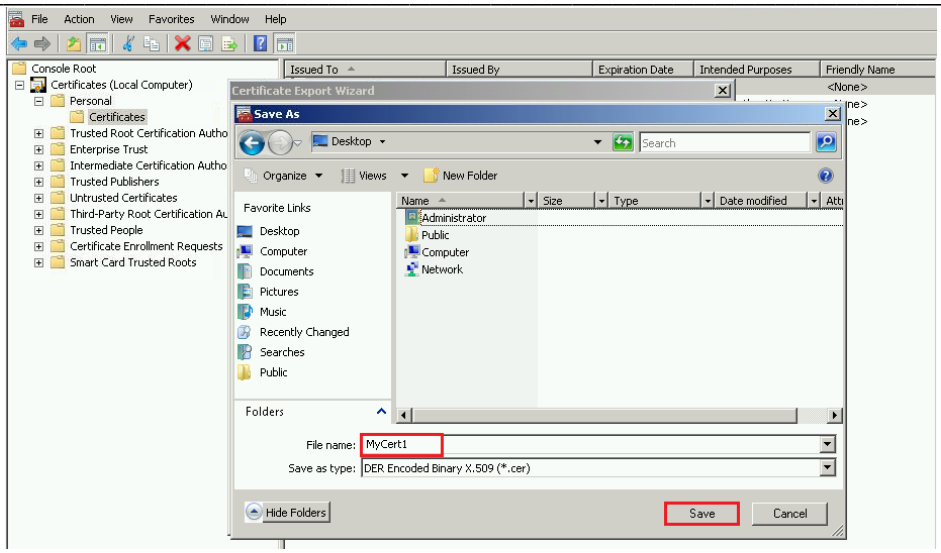


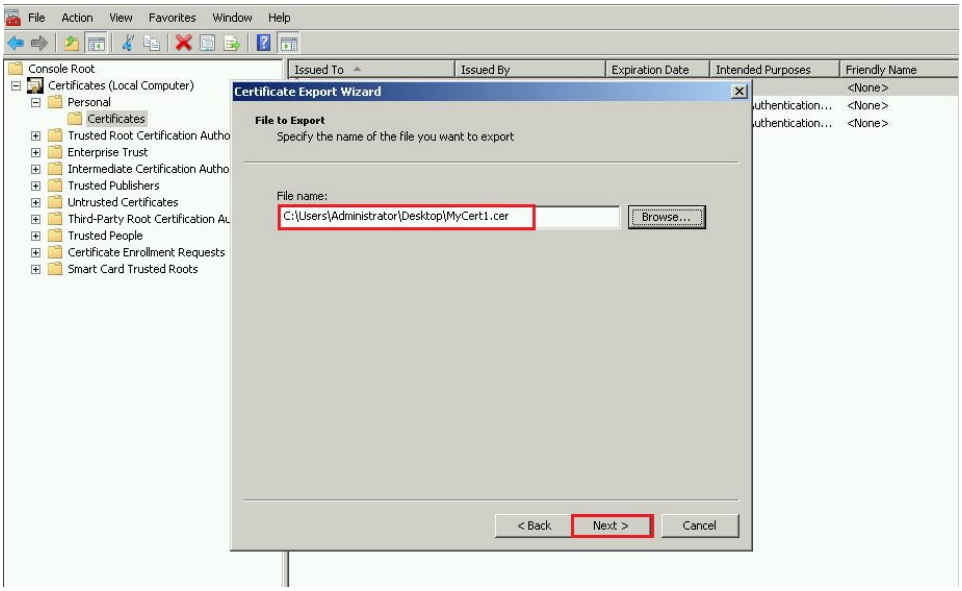

File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Autho
Enterprise Trust
Intermediate Certification Autho
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Au
Trusted People
Certificate Enrollment Requests
Smart Card Trusted Roots
Issued To
Issued By
Expiration Date
Intended Purposes
Friendly Name
<None>
Certificate Export Wizard
Welcome to the Certificate Export Wizard
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

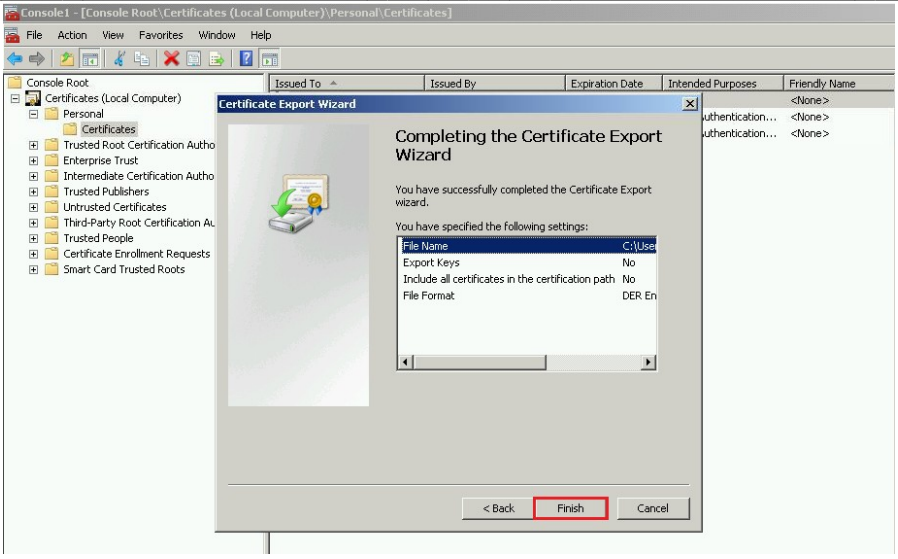

File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Autho
Enterprise Trust
Intermediate Certification Autho
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Au
Trusted People
Certificate Enrollment Requests
Smart Card Trusted Roots
Issued To
Issued By
Expiration Date
Intended Purposes
Friendly Name
<None>
Certificate Export Wizard
Export Private Key
You can choose to export the private key with the certificate.
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.
Do you want to export the private key with the certificate?
Yes, export the private key
No, do not export the private key
Learn more about exporting private keys
< Back
Next >
Cancel

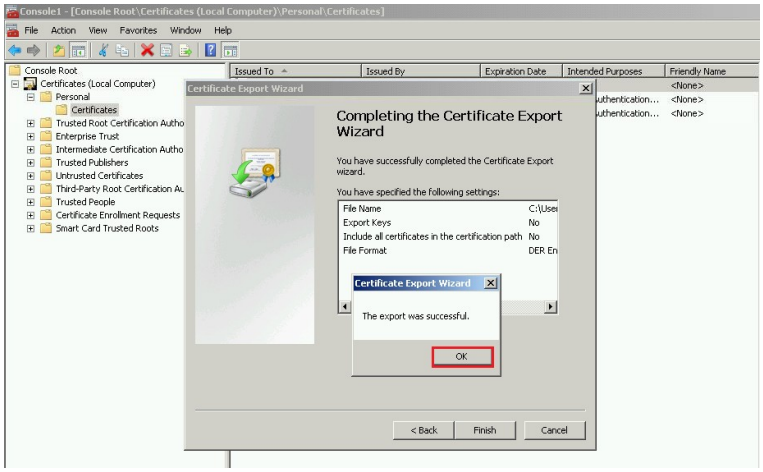

Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Autho
Enterprise Trust
Intermediate Certification Autho
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Au
Trusted People
Certificate Enrollment Requests
Smart Card Trusted Roots
Issued To
Issued By
Expiration Date
Intended Purposes
Friendly Name
<None>
<None>
<None>
Certificate Export Wizard
Export File Format
Certificates can be exported in a variety of file formats.
Select the format you want to use:
DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification path if possible
Personal Information Exchange - PKCS #12 (.PFX)
Include all certificates in the certification path if possible
Delete the private key if the export is successful
Export all extended properties
Microsoft Serialized Certificate Store (.SST)
Learn more about certificate file formats
< Back
Next >
Cancel


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Autho
Enterprise Trust
Intermediate Certification Autho
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Au
Trusted People
Certificate Enrollment Requests
Smart Card Trusted Roots
Issued To
Issued By
Expiration Date
Intended Purposes
Friendly Name
<None>
<None>
<None>
Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
Browse...
< Back
Next >
Cancel

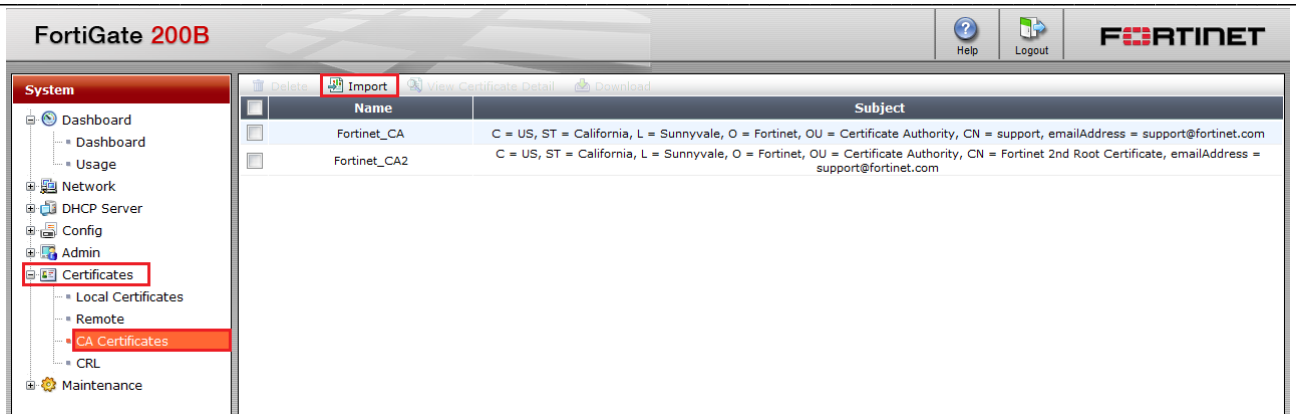

File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Autho
Enterprise Trust
Intermediate Certification Autho
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Au
Trusted People
Certificate Enrollment Requests
Smart Card Trusted Roots
Issued To
Issued By
Expiration Date
Intended Purposes
Friendly Name
Certificate Export Wizard
Save As
Desktop
Search
Organize
Views
New Folder
Favorite Links
Desktop
Computer
Documents
Pictures
Music
Recently Changed
Searches
Public
Name
Size
Type
Date modified
Administrator
Public
Computer
Network
Folders
File name: MyCert1
Save as type: DER Encoded Binary X.509 (*.cer)
Hide Folders
Save
Cancel

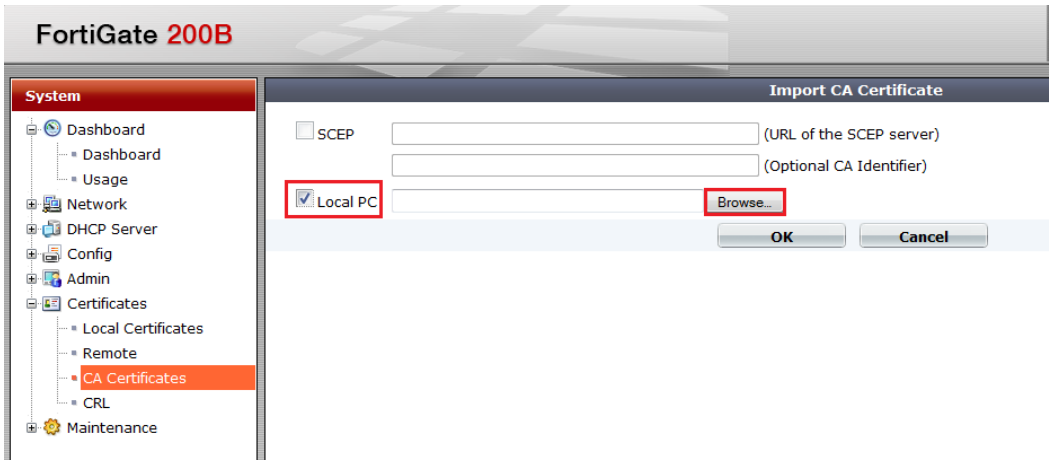

File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Autho
Enterprise Trust
Intermediate Certification Autho
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Au
Trusted People
Certificate Enrollment Requests
Smart Card Trusted Roots
Issued To
Issued By
Expiration Date
Intended Purposes
Friendly Name
<None>
Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
C:\Users\Administrator\Desktop\MyCert1.cer
Browse...
< Back
Next >
Cancel

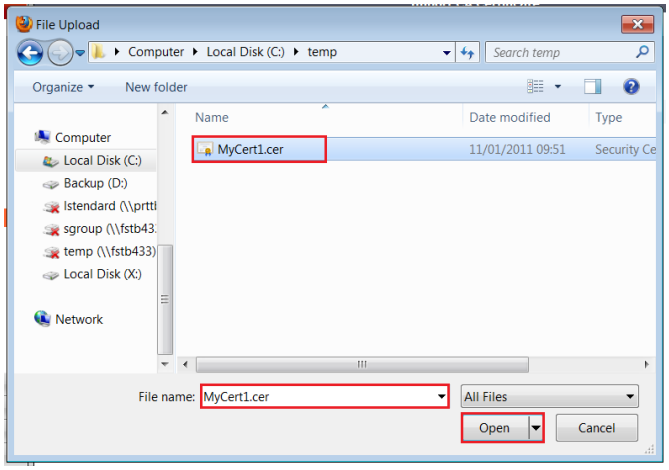


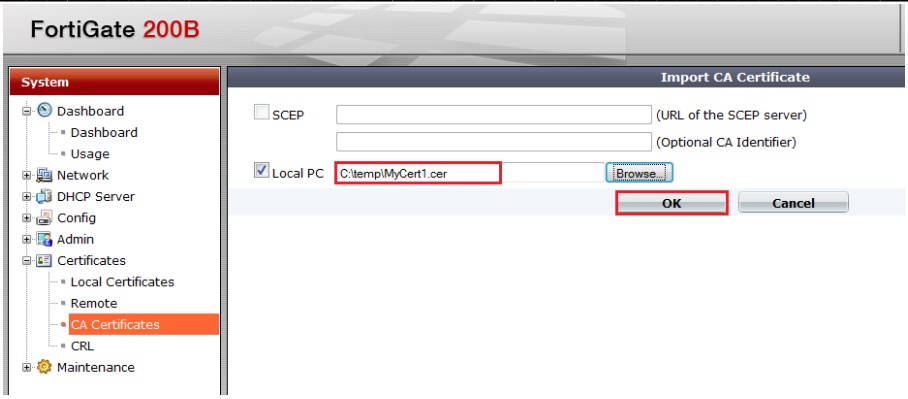


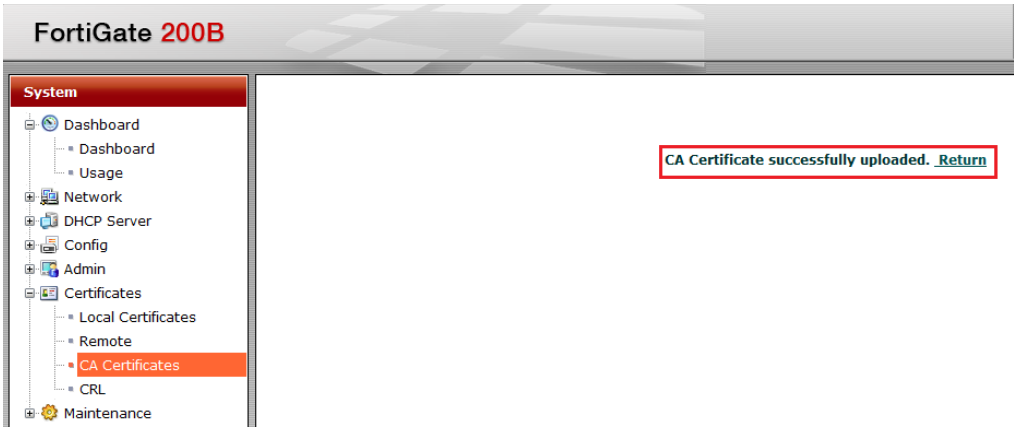
4. Importar o certificado no FortiGate e adicioná-lo à configuração servidor LDAP (Windows AD).


FortiGate 200B
Help
Logout
FORTINET
System
Dashboard
Dashboard
Usage
Network
DHCP Server
Config
Admin
Certificates
Local Certificates
Remote
CA Certificates
CRL
Maintenance
Delete
Import
View Certificate Detail
Download
Name
Subject
Fortinet_CA
C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = support, emailAddress = support@fortinet.com
Fortinet_CA2
C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = Fortinet 2nd Root Certificate, emailAddress = support@fortinet.com

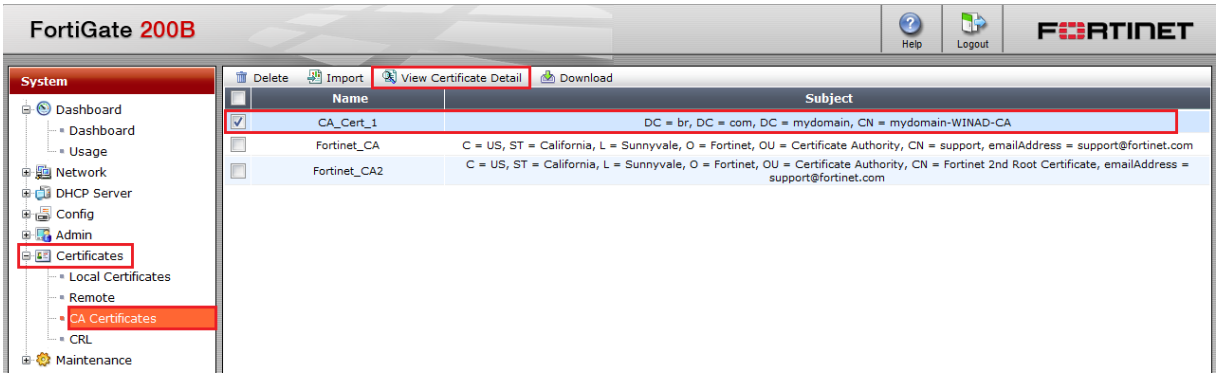

FortiGate 200B
System
Dashboard
Dashboard
Usage
Network
DHCP Server
Config
Admin
Certificates
Local Certificates
Remote
CA Certificates
CRL
Maintenance
Import CA Certificate
SCEP
(URL of the SCEP server)
(Optional CA Identifier)
Local PC
Browse...
OK
Cancel

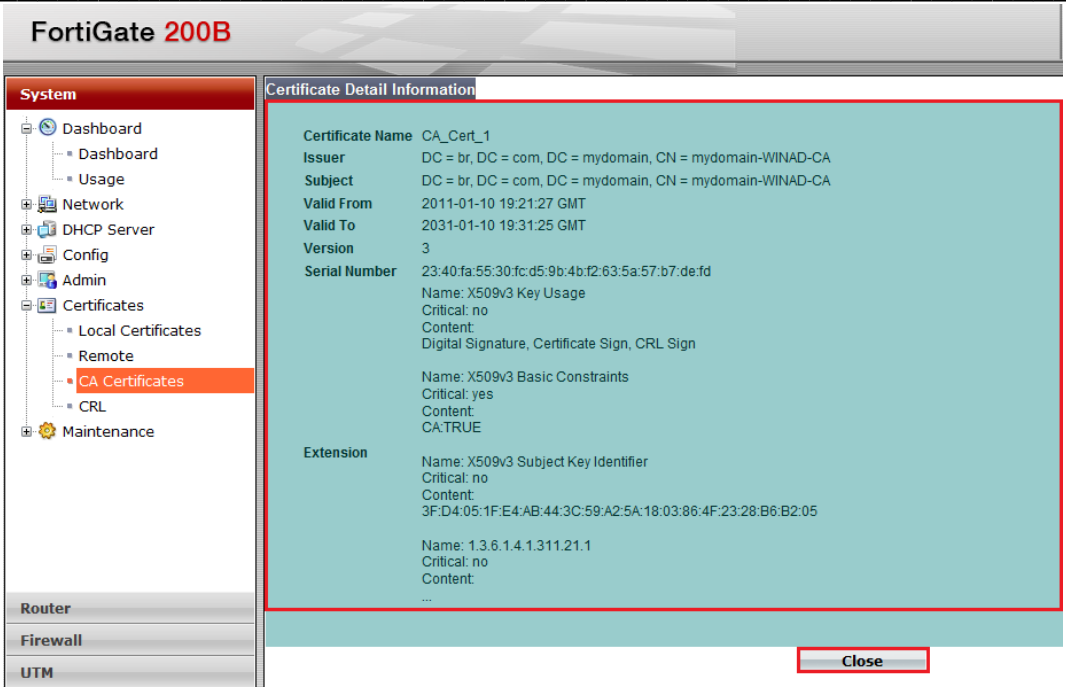

File Upload
Computer
Local Disk (C:)
temp
Search temp
Organize
New folder
Name
Date modified
Type
Computer
Local Disk (C:)
Backup (D:)
lstendard (\\prttl
sgroup (\\fstb43
temp (\\fstb433)
Local Disk (X:)
Network
MyCert1.cer
11/01/2011 09:51
Security Ce
File name:
MyCert1.cer
All Files
Open
Cancel



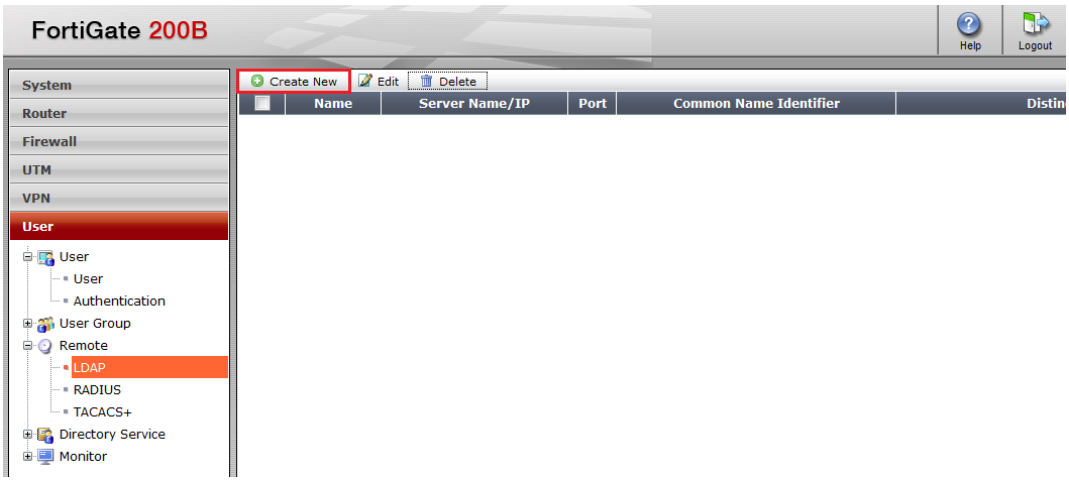


- Pode-se verificar as informações contidas no certificado após a sua importação no FortiGate:





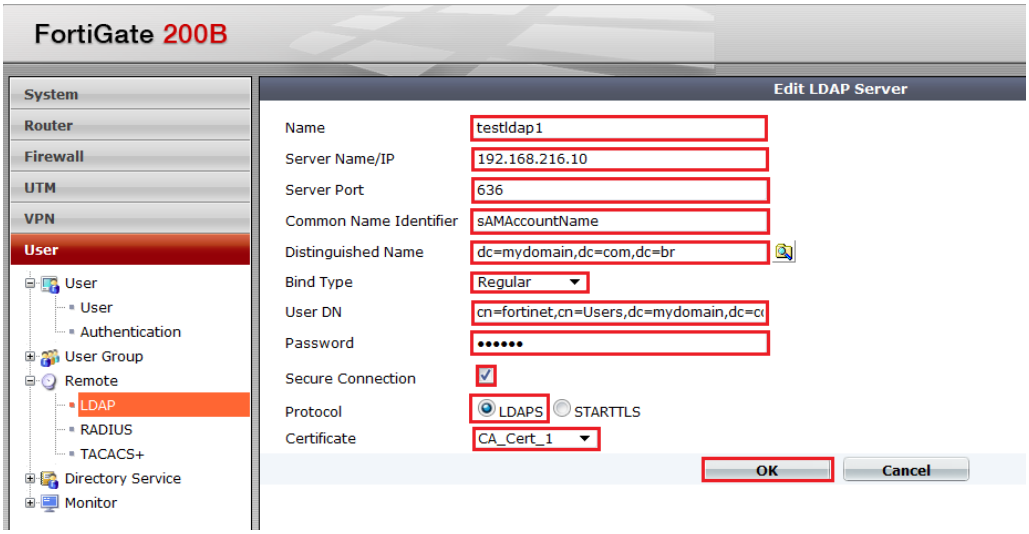
4. Criar um novo servidor LDAP.

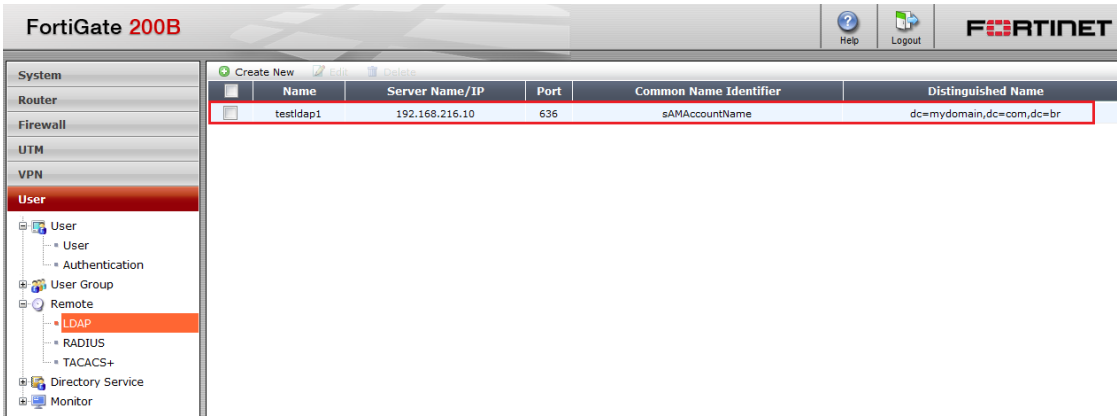


- Para que a comunicação entre o FortiGate ocorra de forma segura (protegida por SSL) deve-se selecionar o protocolo LDAPS e o certificado que foi anteriormente importado.

  No exemplo a seguir o usuário fortinet é um usuário que foi previamente configurado no Windows Active Directory para fazer as queries LDAP. O user DN

(distinguished name) do usuário fortinet é cn=fortinet,cn=Users,dc=mydomain,dc=com,dc=br e ele fará as queries "varrendo" toda a estrutura de árvore abaixo do distinguished name dc=mydomain,dc=com,dc=br.





Agora o servidor LDAP criado (testldap1) pode ser utilizado para autenticar administradores, VPN SSL, VPN IPsec, etc...

6. Testes

Pode-se realizar testes de validação das configurações através da command line (CLI) do FortiGate.

- Habilitar o debug do processo fnbamd com os comandos abaixo:

diagnose debug application fnbamd –1

diagnose debug enable

***Obs**: ao final dos testes deve-se desabilitar o modo debug com o comando “diagnose debug disable”.

- Realizar o teste de autenticação de um usuário do Windows AD com o comando abaixo:
  diagnose test authserver ldap <ldap service> <Windows AD user> <password>
  Uma autenticação com sucesso deve ocorrer como apresentado a seguir:

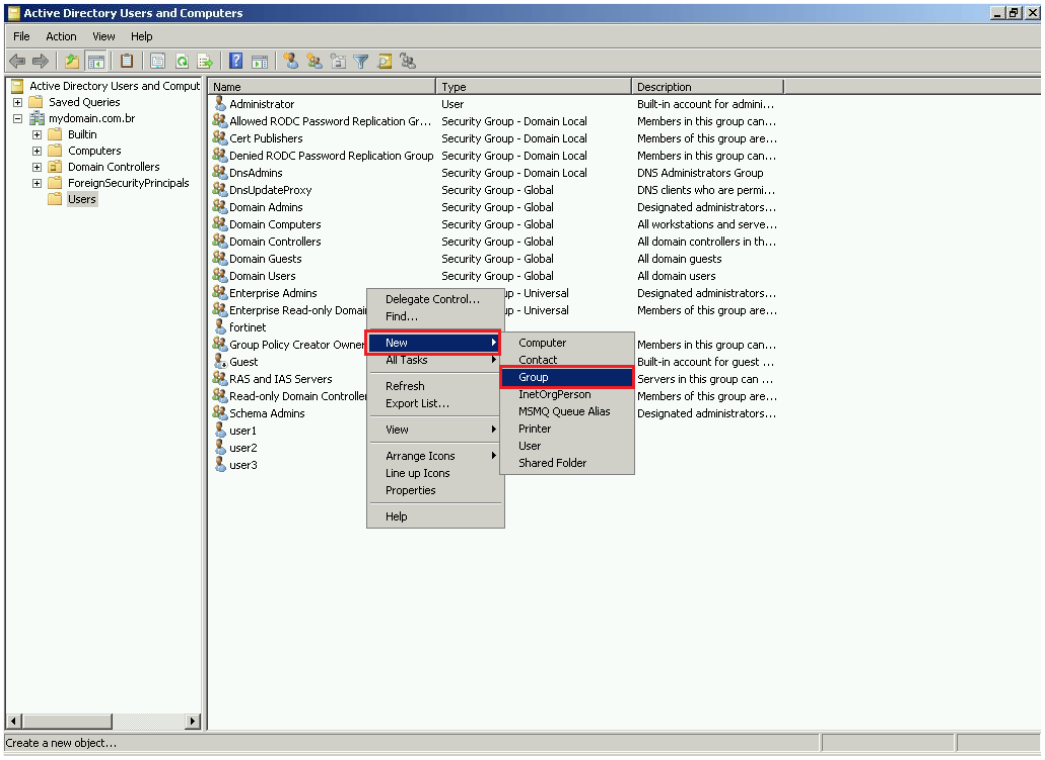
  FG_RENNER_HA1 # **diagnose debug application fnbamd -1**
  FG_RENNER_HA1 # **diagnose debug enable**
  FG_RENNER_HA1 # **diagnose test authserver ldap testldap1 user1 Diveo@123**
  fnbamd_fsm.c[1010] handle_req-Rcvd auth req 29360128 for user1 in testldap1 opt=27 prot=0
  fnbamd_ldap.c[483] resolve_ldap_FQDN-Resolved address 192.168.216.10, result 192.168.216.10
  fnbamd_ldap.c[218] set_cacert_file-CA file: '/etc/cert/ca/CA_Cert_1.cer'
  fnbamd_ldap.c[232] start_search_dn-base:'dc=mydomain,dc=com,dc=br' filter:sAMAccountName=user1
  fnbamd_ldap.c[1179] fnbamd_ldap_get_result-Going to SEARCH state
  fnbamd_fsm.c[1320] poll_ldap_servers-Continue pending for req 29360128
  fnbamd_ldap.c[266] get_all_dn-Found DN 1:CN=user1,CN=Users,DC=mydomain,DC=com,DC=br
  fnbamd_ldap.c[280] get_all_dn-Found 1 DN's
  fnbamd_ldap.c[314] start_next_dn_bind-Trying DN 1:CN=user1,CN=Users,DC=mydomain,DC=com,DC=br
  fnbamd_ldap.c[1217] fnbamd_ldap_get_result-Going to USERBIND state
  fnbamd_fsm.c[1320] poll_ldap_servers-Continue pending for req 29360128
  fnbamd_ldap.c[372] start_multi_attribute_lookup-Adding attr 'memberOf'
  fnbamd_ldap.c[388] start_multi_attribute_lookup-base:'CN=user1,CN=Users,DC=mydomain,DC=com,DC=br' filter:cn=*
  fnbamd_ldap.c[1271] fnbamd_ldap_get_result-Entering CHKUSERATTRS state
  fnbamd_fsm.c[1320] poll_ldap_servers-Continue pending for req 29360128
  fnbamd_ldap.c[1089] fnbamd_ldap_get_result-Not ready yet
  fnbamd_fsm.c[1320] poll_ldap_servers-Continue pending for req 29360128
  fnbamd_ldap.c[415] get_member_of_groups-Get the memberOf groups.
  fnbamd_ldap.c[434] get_member_of_groups-attr='memberOf' - found 0 values
  fnbamd_ldap.c[1285] fnbamd_ldap_get_result-Auth accepted
  fnbamd_ldap.c[1300] fnbamd_ldap_get_result-Going to DONE state res=0
  fnbamd_auth.c[1543] fnbamd_auth_poll_ldap-Result for ldap svr 192.168.216.10 is SUCCESS
  fnbamd_auth.c[1564] fnbamd_auth_poll_ldap-Skipping group matching

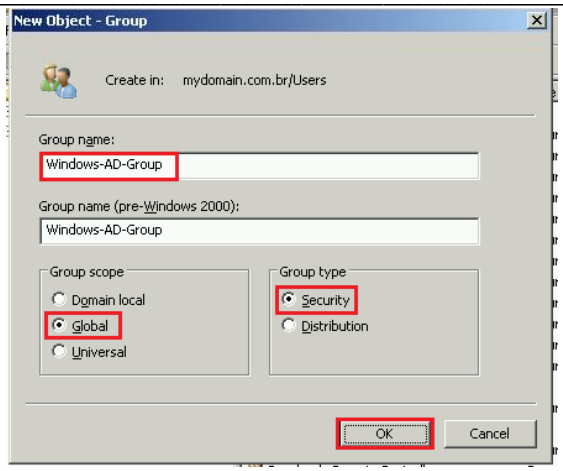
fnbamd_comm.c[112] fnbamd_comm_send_result-Sending result 0 for req 29360128
authenticate 'user1' against 'testldap1' succeeded!
FG_RENNER_HA1 # **diagnose debug disable**
FG_RENNER_HA1 #

Apêndice III – Autenticação no Windows Active Directory com Restrição de Acesso a um Grupo no AD

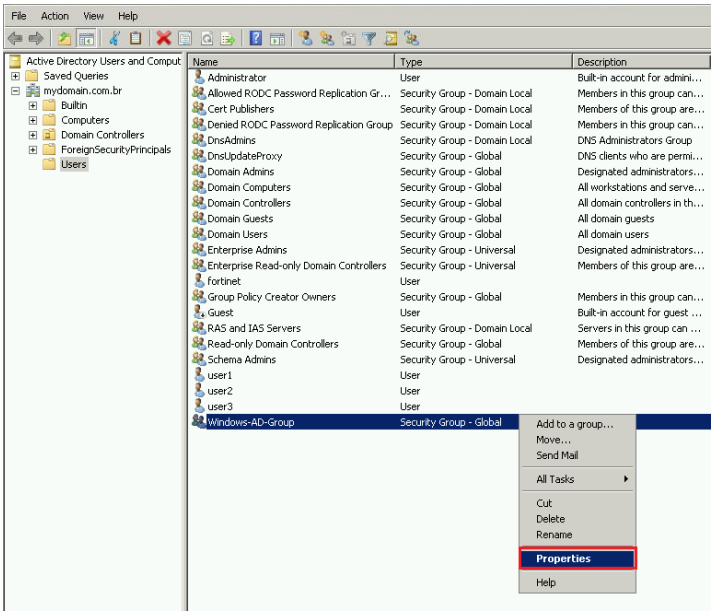
O processo básico de autenticação no Windows AD (sem restrição por grupo) foi apresentado no Apêndice I deste documento. São apresentadas a seguir as configurações adicionais para permitir que apenas os usuários que pertencentes a um determinado grupo do Windows Active Directory possam ser autenticados.

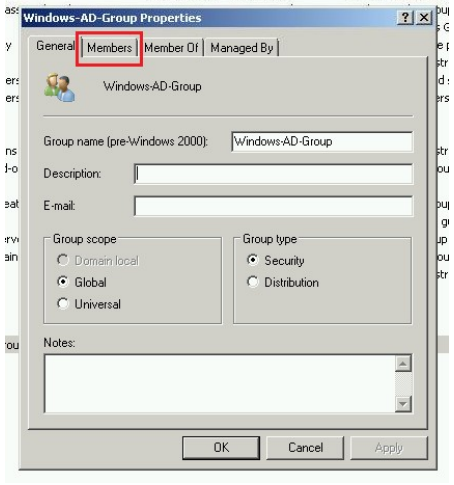
1. Criar um grupo no Windows Active Directory através da Microsoft Management Console "Active Users and Computers".

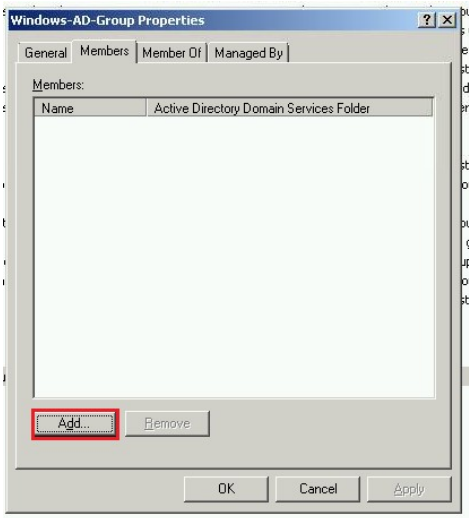


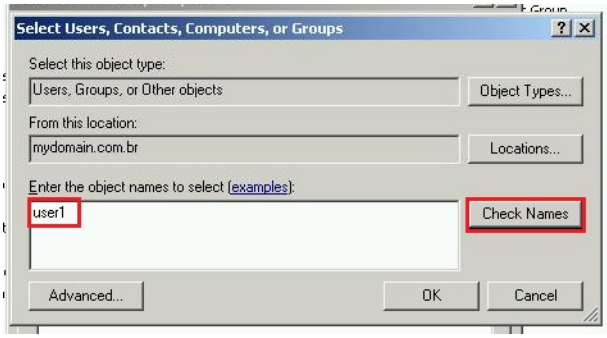


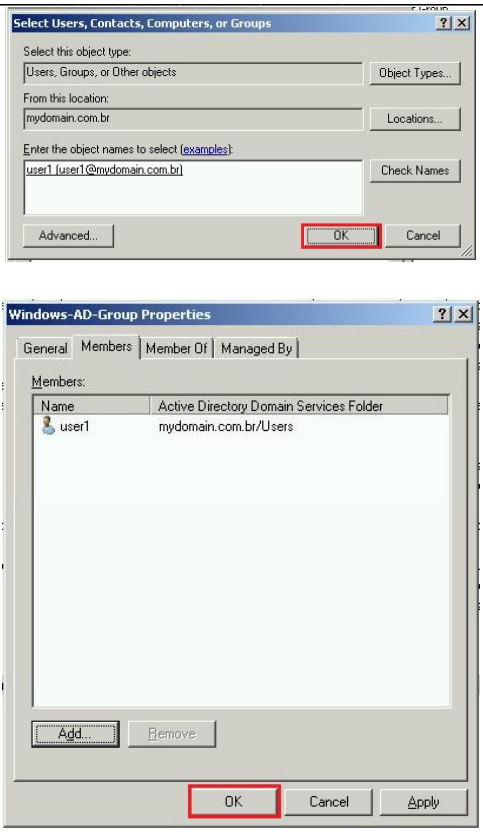
2. Adicionar o usuário desejado ao grupo.



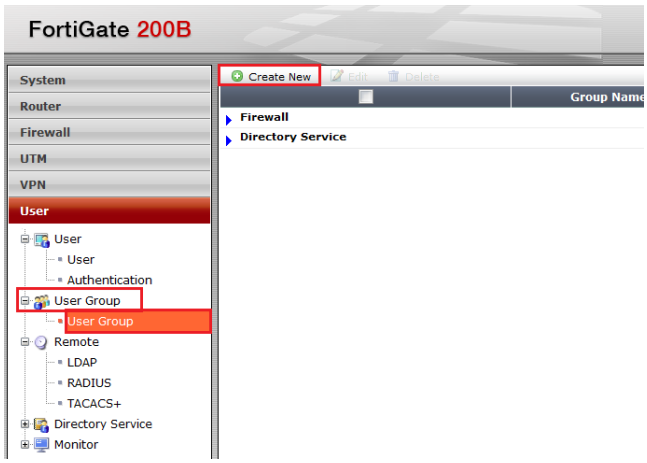

Windows-AD-Group Properties
General
Members
Member Of
Managed By
Windows-AD-Group
Group name (pre-Windows 2000):
Windows-AD-Group
Description:
E-mail:
Group scope
Domain local
Global
Universal
Group type
Security
Distribution
Notes:
OK
Cancel
Apply

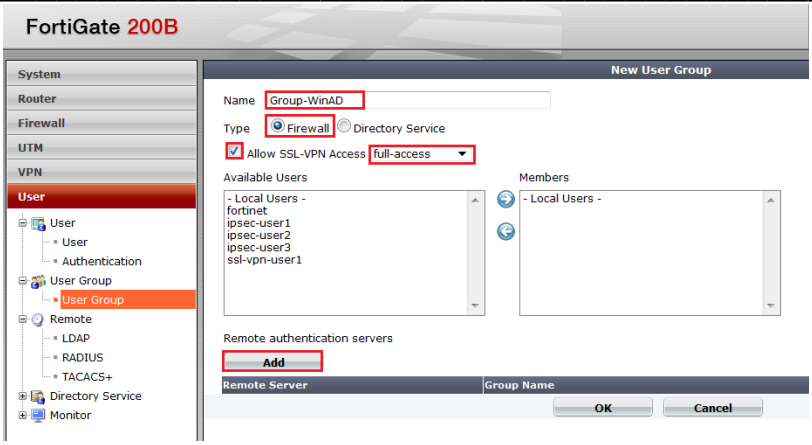

Windows-AD-Group Properties
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
Add...
Remove
OK
Cancel
Apply


Select Users, Contacts, Computers, or Groups
Select this object type:
Users, Groups, or Other objects
Object Types...
From this location:
mydomain.com.br
Locations...
Enter the object names to select (examples):
user1
Check Names
Advanced...
OK
Cancel

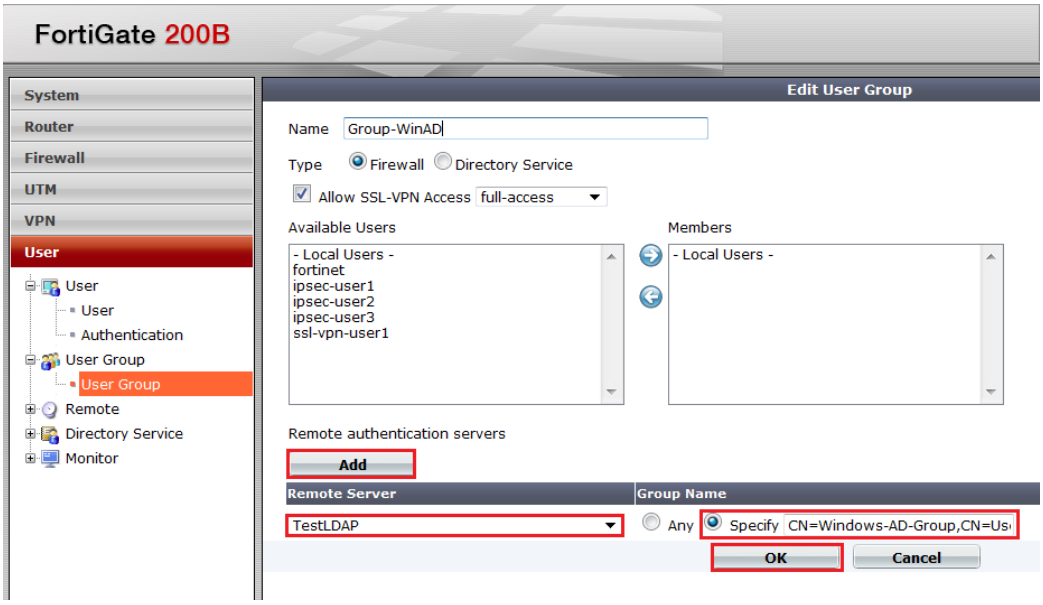


3. Criar um grupo no FortiGate. Associar este grupo ao servidor LDAP que representa o Windows AD.





Especificar o servidor Windows AD no campo Remote Server (ver Apêndice I). Preencher o campo Group Name com o Distinguished Name do grupo no Windows AD. No exemplo o DN é:
CN=Windows-AD-Group,CN=Users,DC=mydomain,DC=com,DC=br



A partir deste momento o grupo Group-WinAD pode ser usado em quaisquer serviços que requeiram autenticação (VPN SSL, VPN IPsec, administradores remotos, etc...).

Exemplo 1: Autenticação do usuário user1 (pertence ao grupo Windows-AD-Group do Windows Active Directory).

```
FG_RENNER_HA1 # diagnose debug application fnbamd -1
FG_RENNER_HA1 # diagnose debug enable

fnbamd_fsm.c[1010] handle_req-Rcvd auth req 3735557 for user1 in Group-WinAD opt=1
prot=9
fnbamd_auth.c[228] radius_start-Didn't find radius servers (0)
fnbamd_auth.c[582] auth_tac_plus_start-Didn't find tac_plus servers (0)
fnbamd_ldap.c[483] resolve_ldap_FQDN-Resolved address 192.168.216.10, result
192.168.216.10
fnbamd_ldap.c[232] start_search_dn-base:'dc=mydomain,dc=com,dc=br'
filter:sAMAccountName=user1

fnbamd_ldap.c[1179] fnbamd_ldap_get_result-Going to SEARCH state
fnbamd_fsm.c[1320] poll_ldap_servers-Continue pending for req 3735557
fnbamd_ldap.c[266] get_all_dn-Found DN
1:CN=user1,CN=Users,DC=mydomain,DC=com,DC=br

fnbamd_ldap.c[280] get_all_dn-Found 1 DN's
fnbamd_ldap.c[314] start_next_dn_bind-Trying DN
1:CN=user1,CN=Users,DC=mydomain,DC=com,DC=br
fnbamd_ldap.c[1217] fnbamd_ldap_get_result-Going to USERBIND state
fnbamd_fsm.c[1320] poll_ldap_servers-Continue pending for req 3735557
fnbamd_ldap.c[372] start_multi_attribute_lookup-Adding attr 'memberOf'
fnbamd_ldap.c[388] start_multi_attribute_lookup-
base:'CN=user1,CN=Users,DC=mydomain,DC=com,DC=br' filter:cn=*

fnbamd_ldap.c[1271] fnbamd_ldap_get_result-Entering CHKUSERATTRS state
fnbamd_fsm.c[1320] poll_ldap_servers-Continue pending for req 3735557
fnbamd_ldap.c[1089] fnbamd_ldap_get_result-Not ready yet
fnbamd_fsm.c[1320] poll_ldap_servers-Continue pending for req 3735557
fnbamd_ldap.c[1089] fnbamd_ldap_get_result-Not ready yet
fnbamd_fsm.c[1320] poll_ldap_servers-Continue pending for req 3735557
fnbamd_ldap.c[1089] fnbamd_ldap_get_result-Not ready yet
fnbamd_fsm.c[1320] poll_ldap_servers-Continue pending for req 3735557
fnbamd_ldap.c[1089] fnbamd_ldap_get_result-Not ready yet
fnbamd_fsm.c[1320] poll_ldap_servers-Continue pending for req 3735557
fnbamd_ldap.c[415] get_member_of_groups-Get the memberOf groups.
fnbamd_ldap.c[439] get_member_of_groups- attr='memberOf', found 1 values
```

fnbamd_ldap.c[446] get_member_of_groups-val[0]='CN=Windows-AD-Group,CN=Users,DC=mydomain,DC=com,DC=br'
fnbamd_ldap.c[1285] **fnbamd_ldap_get_result-Auth accepted**
fnbamd_ldap.c[1300] fnbamd_ldap_get_result-Going to DONE state res=0
fnbamd_auth.c[1543] fnbamd_auth_poll_ldap-Result for ldap svr 192.168.216.10 is SUCCESS
fnbamd_auth.c[1559] fnbamd_auth_poll_ldap-Passed group matching
fnbamd_comm.c[112] fnbamd_comm_send_result-Sending result 0 for req 3735557
fnbamd_fsm.c[1157] handle_req-Rcvd 7 req
fnbamd_cfg.c[397] fnbamd_cfg_get_radius_server-Error finding rad server TestLDAP
fnbamd_acct.c[228] fnbamd_acct_start_START-Error getting radius server
fnbamd_fsm.c[517] create_acct_session-Error start acct type 7
fnbamd_fsm.c[1162] handle_req-Error creating acct session 7

Exemplo 2: Autenticação do usuário user2 (existe no Windows Active Directory mas não pertence ao grupo Windows-AD-Group).

FG_RENNER_HA1 # diagnose debug application fnbamd -1
FG_RENNER_HA1 # diagnose debug enable

fnbamd_fsm.c[1157] handle_req-Rcvd 8 req
fnbamd_cfg.c[397] fnbamd_cfg_get_radius_server-Error finding rad server TestLDAP
fnbamd_acct.c[294] fnbamd_acct_start_STOP-Error getting radius server
fnbamd_fsm.c[517] create_acct_session-Error start acct type 8
fnbamd_fsm.c[1162] handle_req-Error creating acct session 8
fnbamd_fsm.c[1010] handle_req-Rcvd auth req 9961475 for user2 in Group-WinAD opt=1 prot=9
fnbamd_auth.c[228] radius_start-Didn't find radius servers (0)
fnbamd_auth.c[582] auth_tac_plus_start-Didn't find tac_plus servers (0)
fnbamd_ldap.c[483] resolve_ldap_FQDN-Resolved address 192.168.216.10, result 192.168.216.10
fnbamd_ldap.c[232] start_search_dn-base:'dc=mydomain,dc=com,dc=br' filter:sAMAccountName=user2

fnbamd_ldap.c[1179] fnbamd_ldap_get_result-Going to SEARCH state
fnbamd_fsm.c[1320] poll_ldap_servers-Continue pending for req 9961475
fnbamd_ldap.c[266] get_all_dn-Found DN 1:CN=user2,CN=Users,DC=mydomain,DC=com,DC=br

fnbamd_ldap.c[280] get_all_dn-Found 1 DN's
fnbamd_ldap.c[314] start_next_dn_bind-Trying DN 1:CN=user2,CN=Users,DC=mydomain,DC=com,DC=br
fnbamd_ldap.c[1217] fnbamd_ldap_get_result-Going to USERBIND state
fnbamd_fsm.c[1320] poll_ldap_servers-Continue pending for req 9961475

fnbamd_ldap.c[1317] **fnbamd_ldap_get_result-Auth denied**
fnbamd_auth.c[1536] fnbamd_auth_poll_ldap-Result for ldap svr 192.168.216.10 is denied
fnbamd_comm.c[112] fnbamd_comm_send_result-Sending result 1 for req 9961475