

Guia de Referência Rápida

Configuração de VPN entre mGuard e ShrewSoft app

Índice

1.	Introdução.....	3
2.	Cenário utilizado como exemplo neste guia.....	3
3.	Definição dos certificados utilizados na VPN.....	3
4.	Configuração do mGuard.....	4
4.1	Acesso inicial a página Web do mGuard.....	4
4.2	Configuração dos endereços IPs das portas LAN e VLAN.....	5
4.3	Configuração do DNS Dinâmico.....	6
4.4	Importar os certificados do mGuard.....	8
4.5	Configurando a conexão VPN.....	9
5.	Configuração do ShrewSoft VPN Client.....	12
6.	Inicializando e testando a conexão VPN.....	15

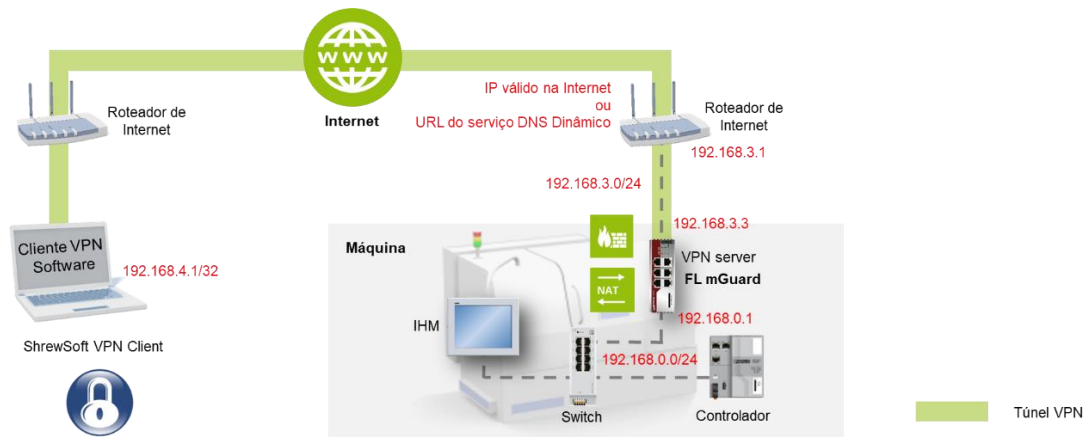
1. Introdução

O objetivo deste guia é apresentar o procedimento de configuração de uma VPN utilizando o protocolo IPsec entre um roteador mGuard e o software ShrewSoft VPN.

2. Cenário utilizado como exemplo neste guia

Para este guia iremos nos basear na topologia apresentada na figura abaixo.

Nesta topologia, o mGuard é o responsável por interligar a máquina e seus dispositivos a rede corporativa. Com o objetivo de realizarmos um acesso remoto a esta máquina, o mGuard será configurado como um servidor VPN, ou seja, ele ficará aguardando a conexão do software cliente VPN, que para esta configuração, será utilizado o software ShrewSoft VPN Client.



Serão considerados os seguintes IPs para esta configuração:

- Rede da máquina : 192.168.0.0 / 255.255.255.0
- Gateway default : 192.168.0.1
- IP do mGuard
 - LAN : 192.168.0.1
 - WAN : 192.168.3.3 / Gateway Default: 192.168.3.1
- Virtual IP do ShrewSoft : 192.168.4.1 / 255.255.255.255

Neste tutorial, será utilizado o roteador mGuard modelo TC MGuard RS4000 4G VPN (2903586). Porém, as configurações valem para todos os demais modelos com suporte a VPN.

3. Definição dos certificados utilizados na VPN

Nesta configuração da VPN, utilizaremos o protocolo IPsec. O método de autenticação entre o servidor e o cliente será realizado através de certificados X.509.

Desta forma, será necessário a criação dos certificados específicos para cada equipamento.

Para esta aplicação serão necessários os seguintes certificados:

- mGuard Server
 - Certificado CA
 - Formato: PEM
 - Nome neste guia: Certificado_CA.crt
 - Certificado de máquina
 - Formato: PKC#12
 - Nome neste guia: mGuard_Server.pfx

- ShrewSoft VPN Client
 - Certificado CA (o mesmo certificado do mGuard)
 - Formato: PEM
 - Nome neste guia: Certificado_CA.crt
 - Certificado de máquina
 - Formato: PEM
 - Nome neste guia: ShrewSoft_Client.crt
 - Certificado de máquina com chave privada
 - Formato: PEM + Chave
 - Nome neste guia: ShrewSoft_Client.pem

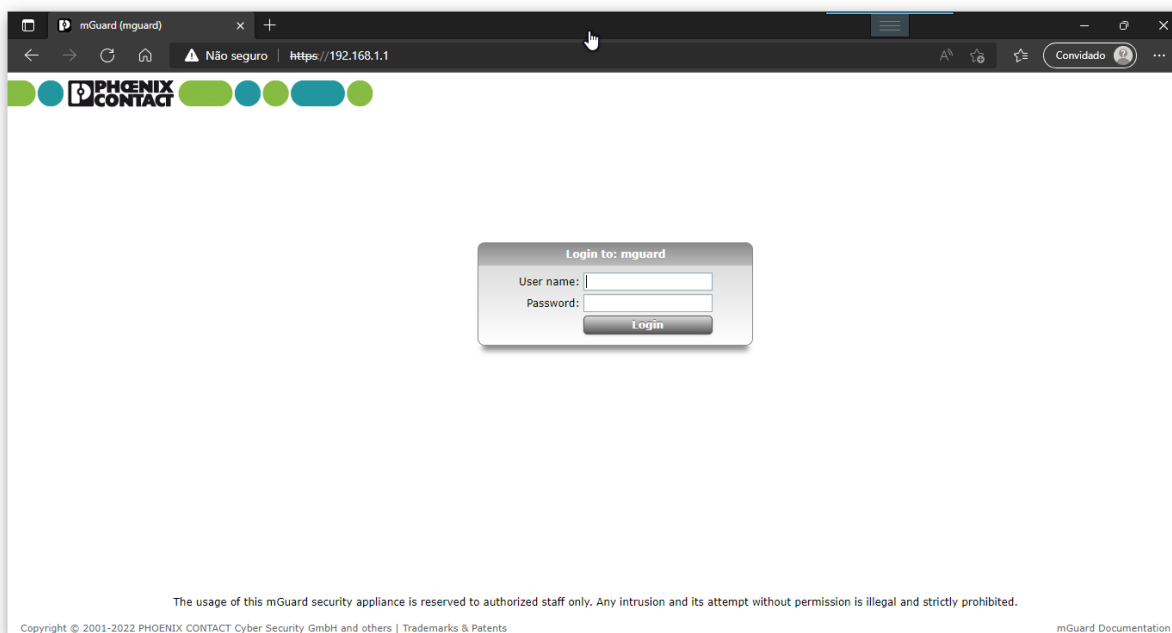
Para a criação dos certificados, consulte o guia **QRG_VPN_Criar_Certificados_X509**.

4. Configuração do mGuard

4.1 Acesso inicial a página Web do mGuard

Na configuração de fábrica, o endereço da porta LAN do mGuard está configurada com o endereço IP 192.168.1.1.

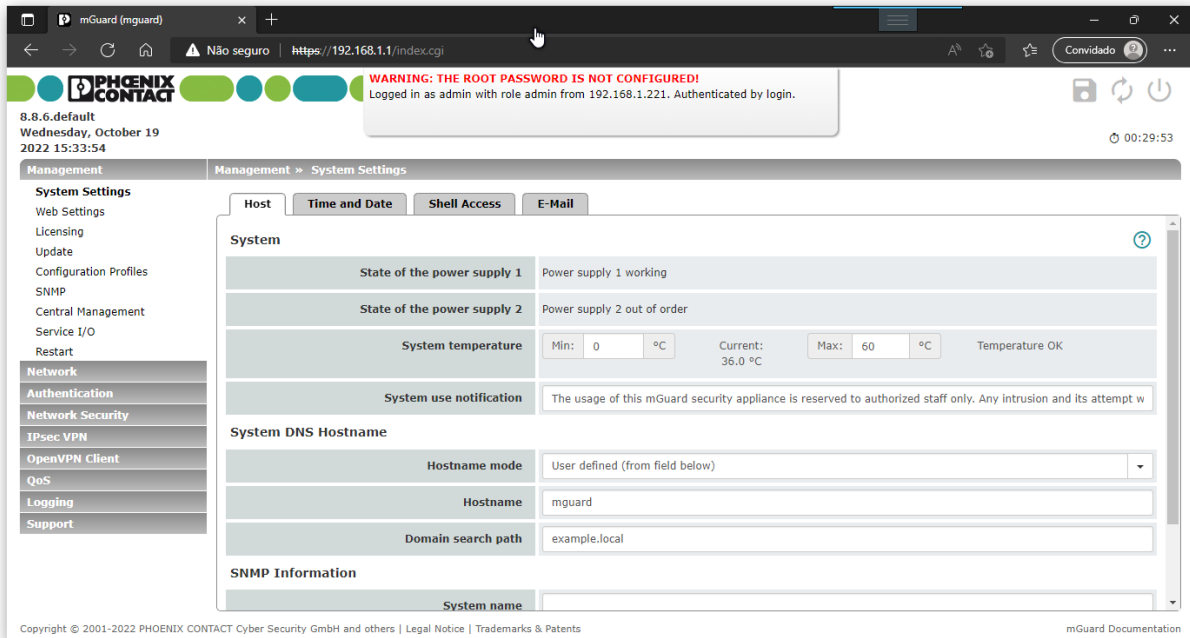
- a) Para acessar a página web, digite <https://192.168.1.1> no navegador Web. A página de login será aberta.



- b) Digite o usuário e senha. Os valores padrões de fábrica são:

Usuário: admin
Senha: mGuard

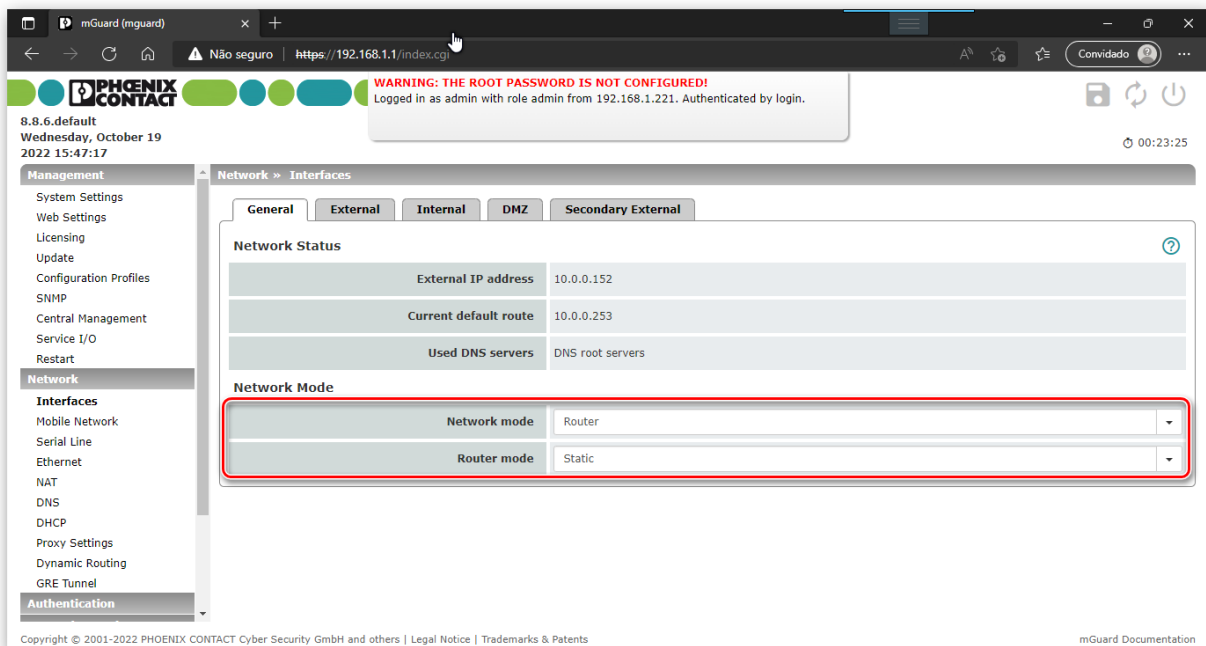
A página de configuração inicial será mostrada.



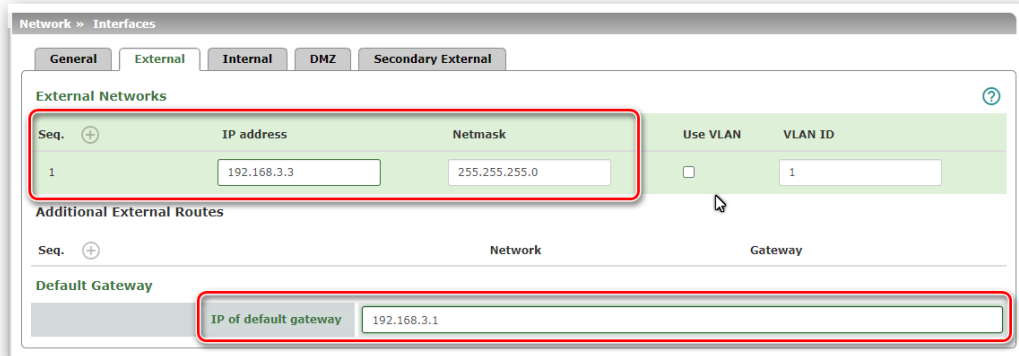
4.2 Configuração dos endereços IPs das portas LAN e WAN

Para configurar os endereços IPs do mGuard, siga os seguintes passos:

- Acesse, no menu da esquerda, a opção **Network > Interfaces**.
- Nesta tela, selecione as opções mostradas na tela abaixo.
Neste tutorial iremos definir um endereço fixo para a porta WAN (porta externa). Porém é possível definir a opção DHCP em Router Mode, a fim de obter um IP automaticamente pela rede ao qual o mGuard será conectado.



- c) Selecione a aba **External** para configurar o endereço IP da porta WAN. Defina o endereço IP da porta e o endereço do Gateway Default da rede (endereço do roteador da rede).



Network » Interfaces

General External Internal DMZ Secondary External

External Networks

Seq.	IP address	Netmask	Use VLAN	VLAN ID
1	192.168.3.3	255.255.255.0	<input type="checkbox"/>	1

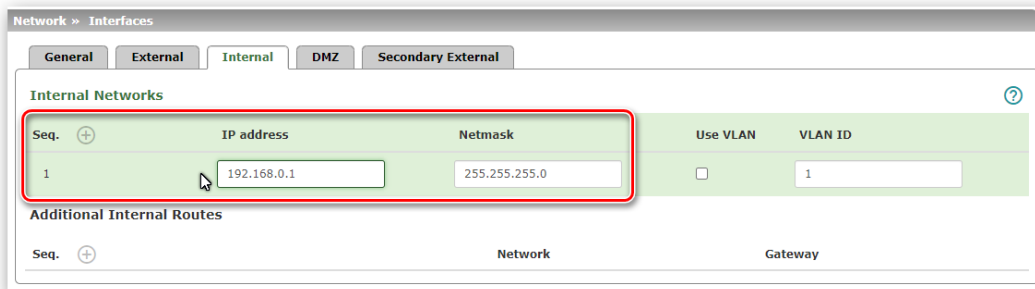
Additional External Routes

Seq.	Network	Gateway

Default Gateway

IP of default gateway: 192.168.3.1

- d) Selecione a aba **Internal** para configurar o endereço IP da porta LAN.



Network » Interfaces

General External Internal DMZ Secondary External

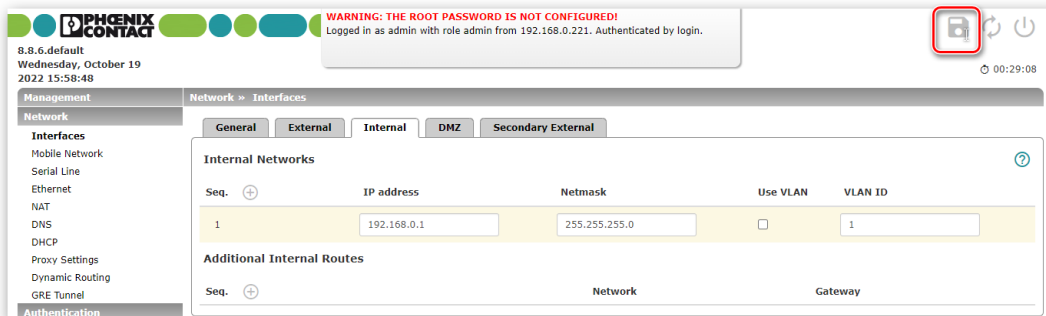
Internal Networks

Seq.	IP address	Netmask	Use VLAN	VLAN ID
1	192.168.0.1	255.255.255.0	<input type="checkbox"/>	1

Additional Internal Routes

Seq.	Network	Gateway

- e) Clique no ícone superior no formato de um disquete, para salvar a configuração.



8.8.6.default
Wednesday, October 19
2022 15:58:48

WARNING: THE ROOT PASSWORD IS NOT CONFIGURED!
Logged in as admin with role admin from 192.168.0.221. Authenticated by login.

00:29:08

Management

Network » Interfaces

General External Internal DMZ Secondary External

Internal Networks

Seq.	IP address	Netmask	Use VLAN	VLAN ID
1	192.168.0.1	255.255.255.0	<input type="checkbox"/>	1

Additional Internal Routes

Seq.	Network	Gateway

Neste momento, o mGuard irá assumir as novas configurações de IP das portas. Portanto para voltar a acessar a página de configuração é necessário alterar o endereço IP da porta do computador para a nova faixa de IP (ex: 192.168.0.xx) e digitar no navegador Web, o novo endereço IP (<https://192.168.0.1>).

4.3 Configuração do DNS Dinâmico

Neste tutorial, o mGuard será configurado como um Servidor VPN. Desta forma, ele fica aguardando o Cliente VPN iniciar a conexão.

Para o Cliente VPN encontrar o mGuard através da internet, é necessário termos um endereço IP válido na internet que dê acesso ao mGuard. Neste caso, podemos ter 2 situações:

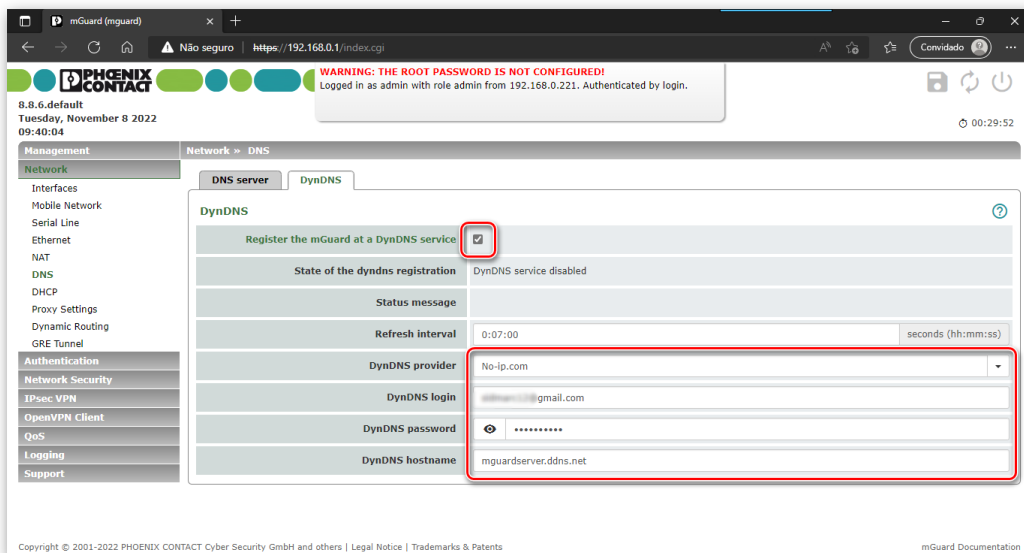
- 1) mGuard conectado via porta WAN na rede interna da empresa e acesso a internet via roteador de Internet da empresa (conforme apresentado na topologia do capítulo 2).
- 2) mGuard se comunica diretamente na internet através de um modem celular incorporado a ele (Ex: TC MGuard RS4000 4G VPN).

Nos dois casos, podemos ter endereços IPs fixos ou dinâmicos. No caso da empresa, esta pode ter um IP fixo contratada pela fornecedora do link de internet ou pode ter um IP dinâmico onde a cada momento recebe um IP diferente para acesso à internet. No caso do modem celular temos as duas opções também. SIM Card com IP fixo contratado junto a empresa de telefonia celular ou um SIM Card tradicional com IP dinâmico.

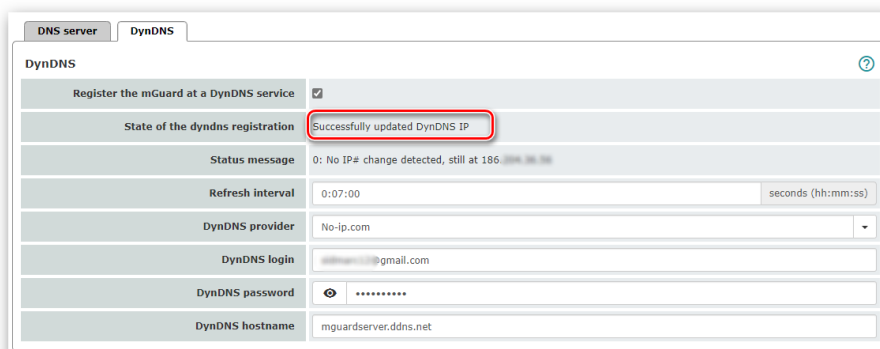
No caso de IPs fixos, basta informamos este IP no ShrewSoft para que ele encontre mGuard. No caso de IP dinâmico devemos utilizar algum serviço de DNS Dinâmico para que possamos encontrar o mGuard usando uma URL.

Para utilizarmos um serviço de DNS dinâmico com o mGuard, devemos seguir os seguintes passos:

- Acesse, no menu da esquerda, a opção **Network > DNS**. Selecione a aba **DynDNS**.
- Nesta aba, habilite o serviço, escolha o serviço a ser usado (neste tutorial usaremos o no-ip), insira seu usuário e senha da sua conta no serviço de DNS dinâmico e o hostname criado neste serviço.
- Clique no ícone superior no formato de um disquete, para salvar a configuração.



Verifique se o mGuard conseguiu conectar ao serviço DNS e atualizar seu IP.



Nota: Direcionamento de porta no roteador de Internet

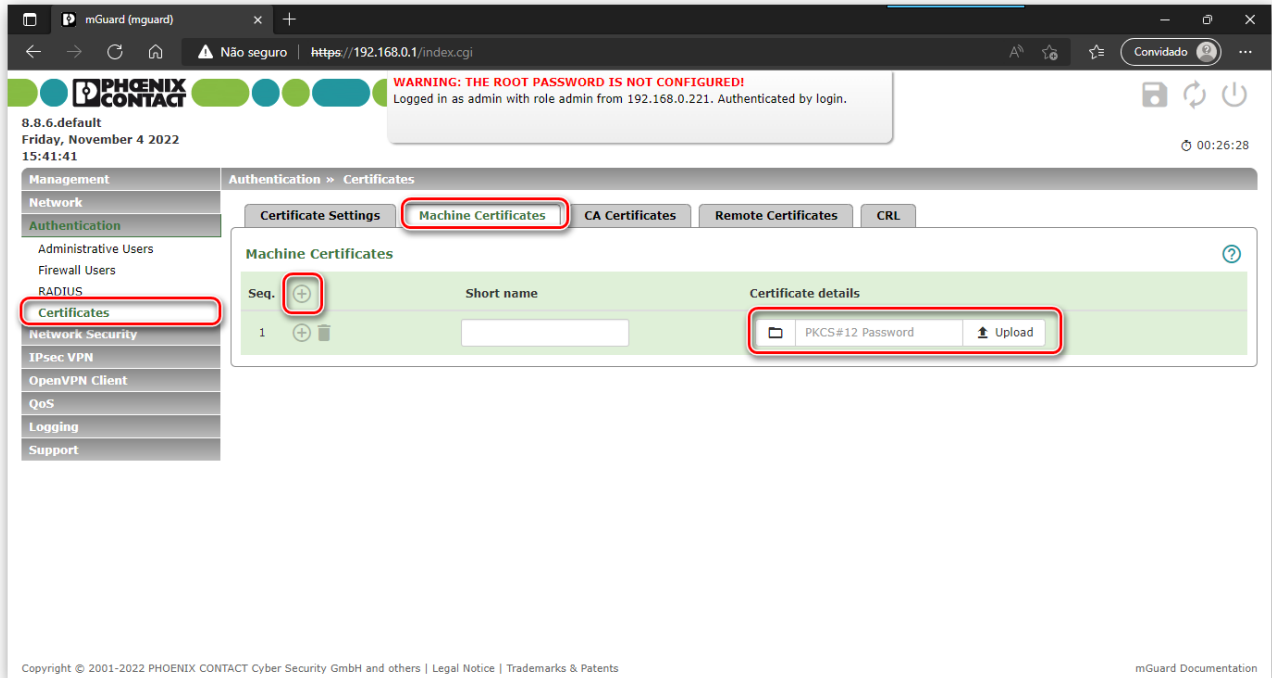
Caso o mGuard esteja sendo usado na rede interna da empresa (Situação 1 acima), é necessário realizar um direcionamento de portas para que a comunicação do Cliente VPN que chega pela IP do roteador de internet seja direcionado diretamente para o mGuard. Esta configuração deve ser feita no roteador de internet pela equipe de TI da empresa, conforme exemplo abaixo:



IP and Port Forwarding						
Protocol	From IP	From port	Incoming on IP	Incoming on port	Redirect to IP	Redirect to port
UDP	0.0.0.0/0	any	%extern	500	192.168.3.3	500
UDP	0.0.0.0/0	any	%extern	4500	192.168.3.3	4500

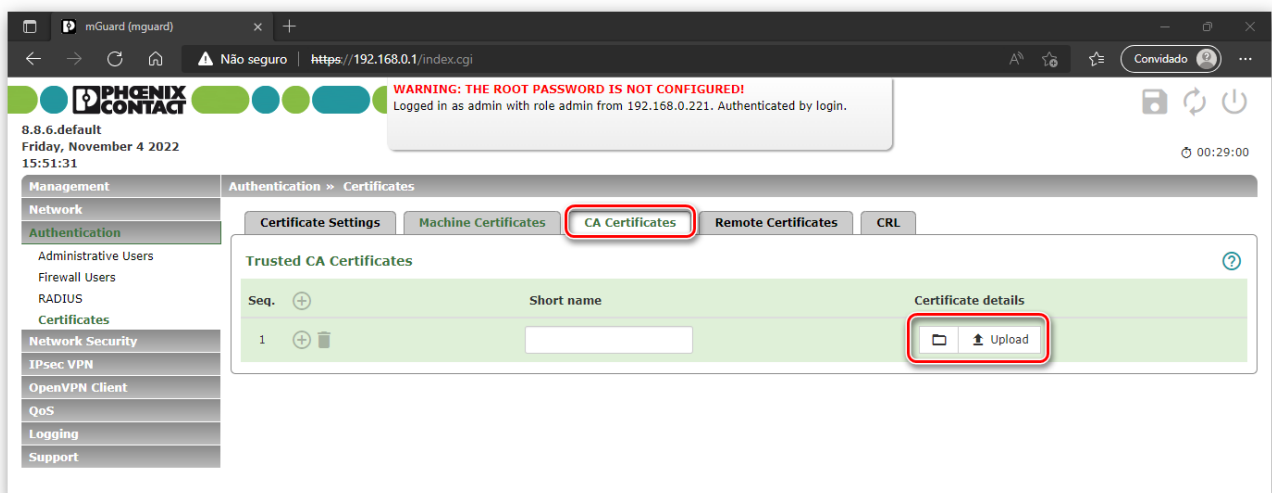
4.4 Importar os certificados do mGuard


Nesta etapa, importaremos o certificado CA e o certificado de máquina no mGuard através dos seguintes passos:

- a) Acesse, no menu da esquerda, a opção **Authentication > Certificates**. Selecione a aba **Machine Certificates**



- b) Clique no ícone  para adicionar um certificado.
- c) Clique no ícone  para selecionar o certificado de máquina (neste guia chamado de mGuard_Server.pfx) e insira a senha definida na criação do certificado. Clique em **upload**. Confira o certificado clicando na seta ao lado de **upload**.
- d) Clique na aba **CA Certificates**

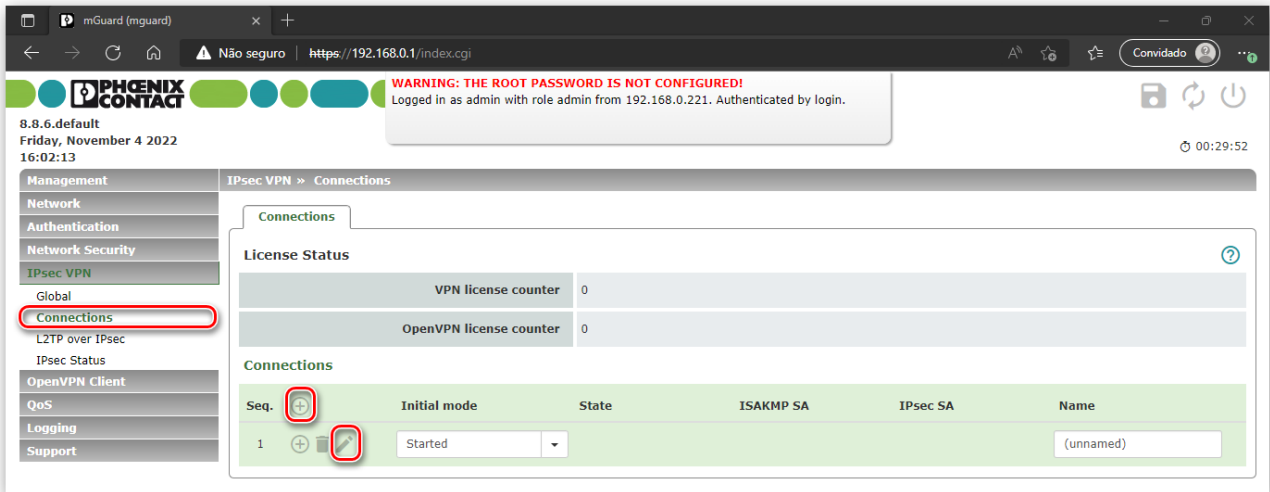




- e) Clique no ícone  para selecionar o certificado CA (neste guia chamado de Certificado_CA.crt) e clique em **upload**. Confira o certificado clicando na seta ao lado de **upload**.

4.5 Configurando a conexão VPN

Nesta etapa, iremos criar e configurar a conexão VPN. Para isto, siga os seguintes passos:

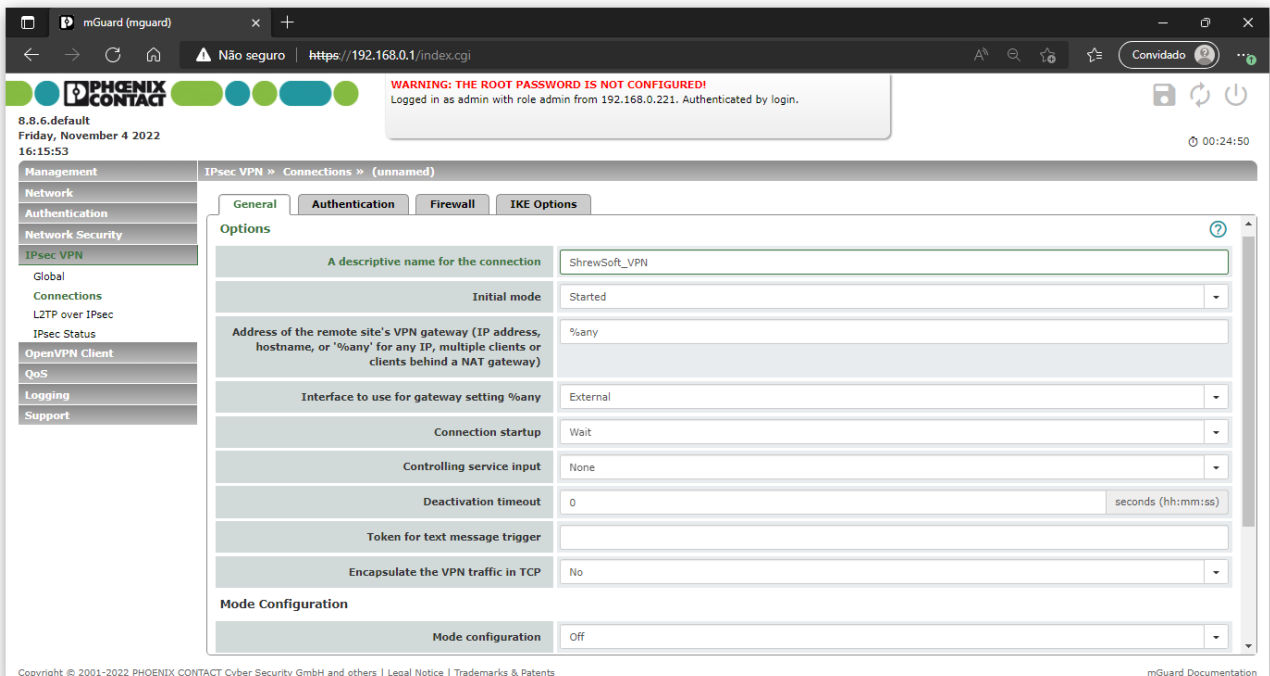
a) Acesse, no menu da esquerda, a opção **IPsec VPN > Connections**.



b) Clique no ícone  para adicionar uma configuração de VPN e clique no ícone  para entrar na edição da VPN.

c) Na tela que abrirá, defina o nome da VPN em **“A descriptive name for the connection”**.

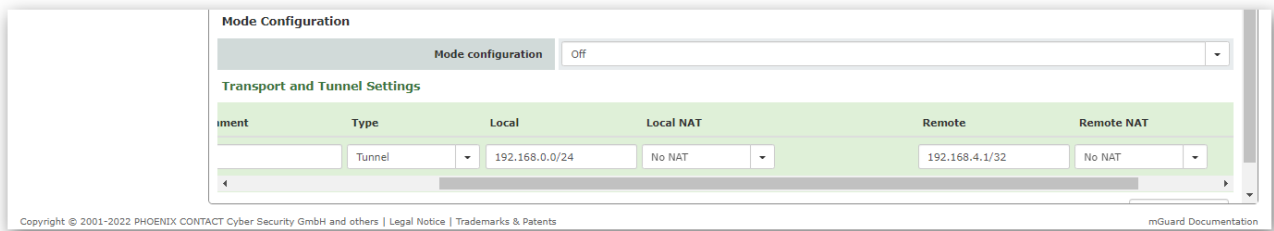
d) Em seguida, defina os parâmetros conforme mostrado na figura abaixo.



Observe:


- em **Connection startup** foi definido como “Wait”, pois o mGuard será o Servidor VPN, o qual aguarda uma conexão do Cliente VPN.
- em **Interface to use for gateway setting %any** foi definido como “External” indicando que a conexão será feita pela porta WAN do mGuard.

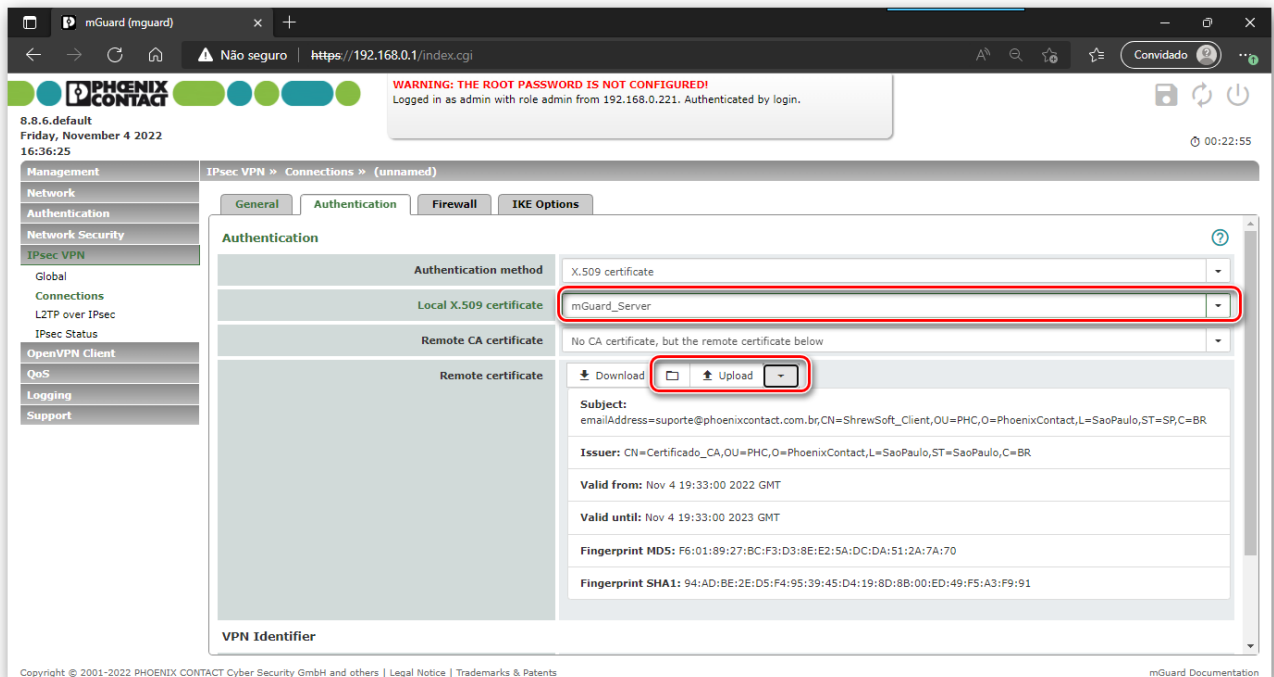
- e) Em **Transport and Tunnel Settings** defina os parâmetros da rede local e remota, conforme mostrado na figura abaixo.



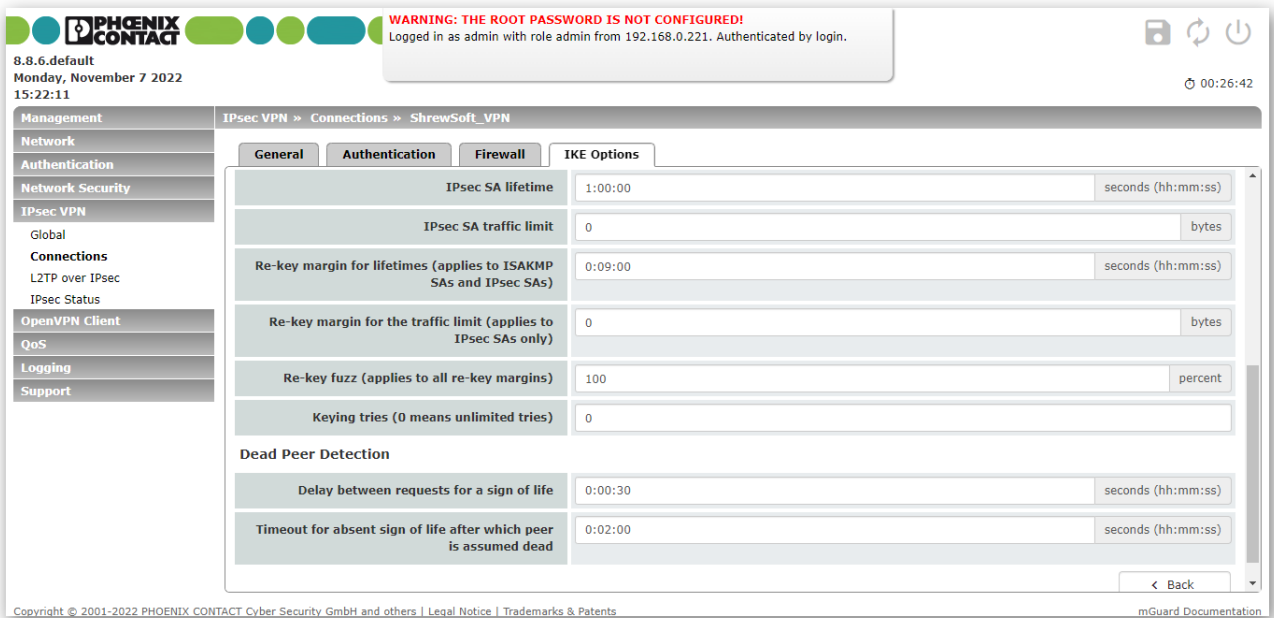
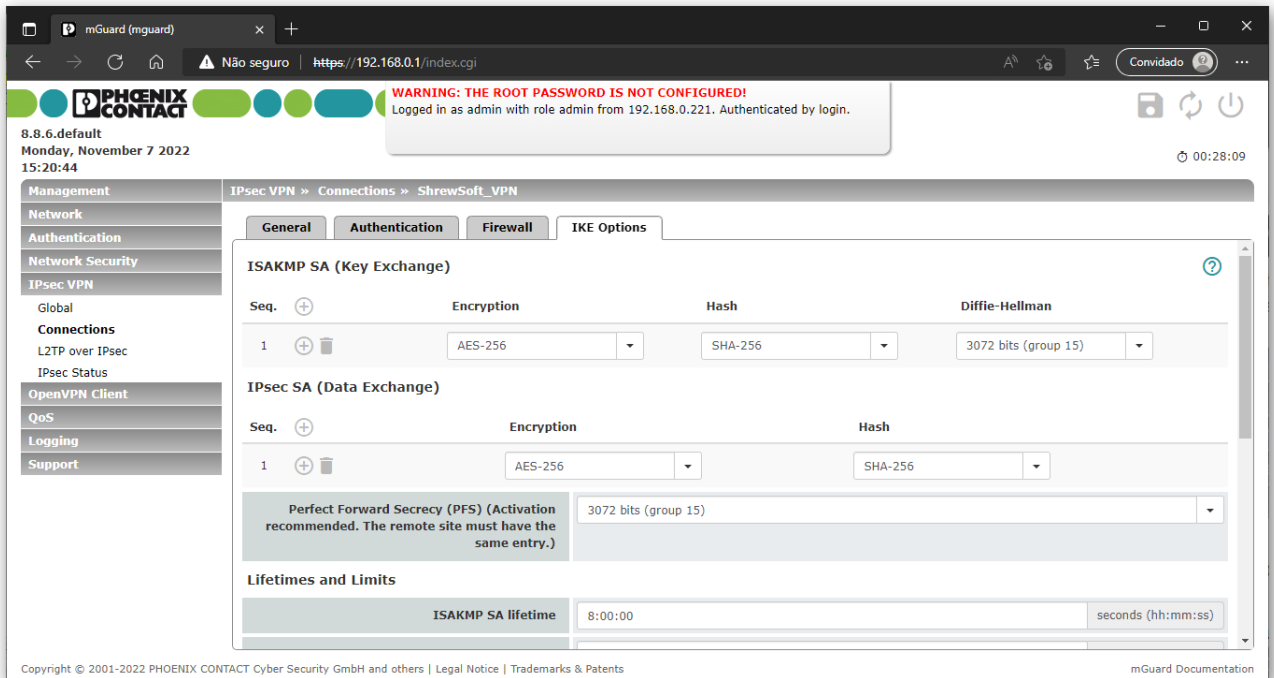
- Type: Tunnel
- Local: 192.168.0.0/24
- Remote: 192.168.4.1/32

- f) Mude para a aba **Authentication**.

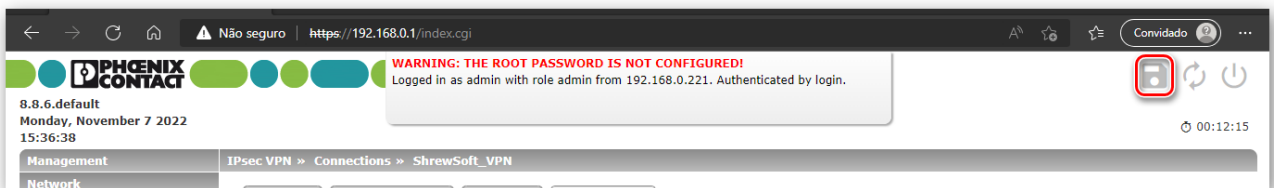
- Defina **Authentication Method** para X.509 Certificate.
- Selecione em **Local X.509 certificate** o certificado de máquina já carregado (mGuard_Server).
- Defina **Remote CA Certificate** para **"No CA certificate, but the remote certificate below"**.
- Clique no ícone  para selecionar o certificado de máquina do ShrewSoft (neste guia chamado de ShrewSoft_Client.crt) e clique em **upload**. Confira o certificado clicando na seta ao lado de **upload**.



- g) Mude para a aba **IKE Options**. Ajuste os parâmetros desta janela conforme mostrado nas figuras abaixo. Os valores abaixo são apenas sugestões. Porém estes valores devem coincidir exatamente com os valores que serão configurados no software ShrewSoft VPN Client.



h) Salve a configuração realizada clicando no ícone no formato de “disquete” no canto direito superior da tela.

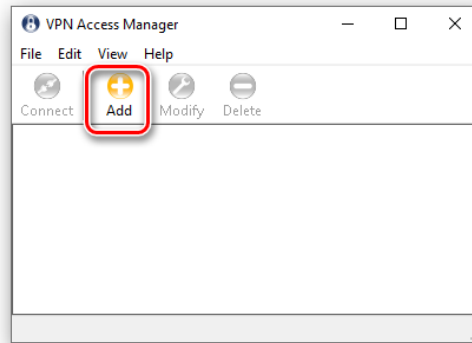


Com isto, concluímos a configuração da VPN no mGuard.

5. Configuração do ShrewSoft VPN Client

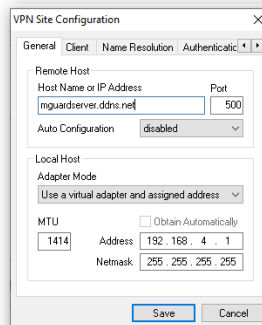
Para criarmos uma conexão VPN com o ShrewSoft VPN Client siga os seguintes passos:

a) Abra o software ShrewSoft e clique no botão **Add**.

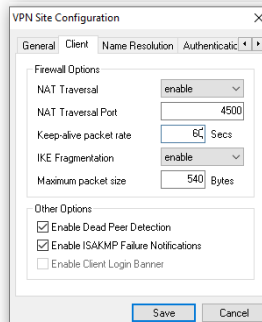


b) Na aba **General**, configure os seguintes parâmetros:

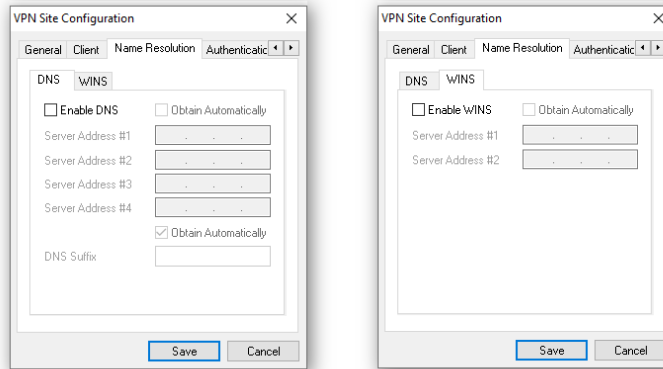
- **Host Name or IP Address:** entre com o endereço IP público do mGuard ou a URL configurada no serviço DNS dinâmico.
- **Auto Configuration:** selecionar **disabled**.
- **Address Method:** selecionar **Use a virtual adapter and assigned address**.
- **MTU:** 1414.
- **Address/Netmask:** entre com o endereço IP Virtual do cliente VPN. Neste tutorial foi definido como 192.168.4.1 / 255.255.255.255.



c) Na aba **Client**, configure os parâmetros conforme figura abaixo.

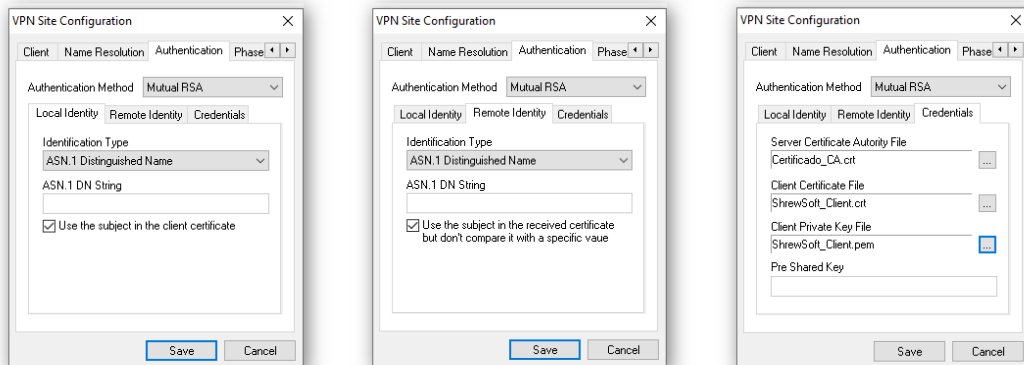


d) Na aba **Name Resolution**, desabilite todas as opções.

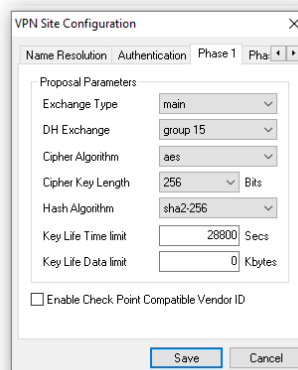


e) Na aba **Authentication**, configure da seguinte forma:

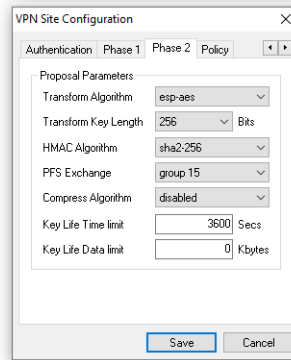
- **Authentication Method:** selecione **Mutual RSA**.
- Nas abas Local Identity and Remote Identity, configure conforme figuras abaixo.
- Na aba Credentials, selecione os certificados criados para o ShrewSoft
 - **Server Certificate Authority File:** selecione o certificado CA (neste guia chamado de Certificado_CA.crt).
 - **Client Certificate File:** selecione o certificado de máquina (neste guia chamado de ShrewSoft_Client.crt).
 - **Client Private Key File:** selecione o certificado de máquina com chave privada (neste guia chamado de ShrewSoft_Client.pem).



f) Na aba **Phase 1**, configure os parâmetros conforme figura abaixo.

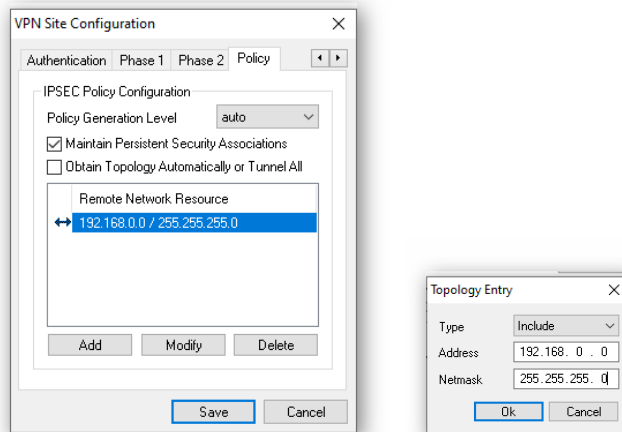


g) Na aba **Phase 2**, configure os parâmetros conforme figura abaixo.



h) Na aba **Policy**, configure da seguinte forma:

- Ative a opção **Maintain Persistent Security Associations**.
- Clique Add e entre com a rede interna do mGuard. Neste tutorial foi definido como 192.168.0.1 / 255.255.255.0.
- Clique **OK**.



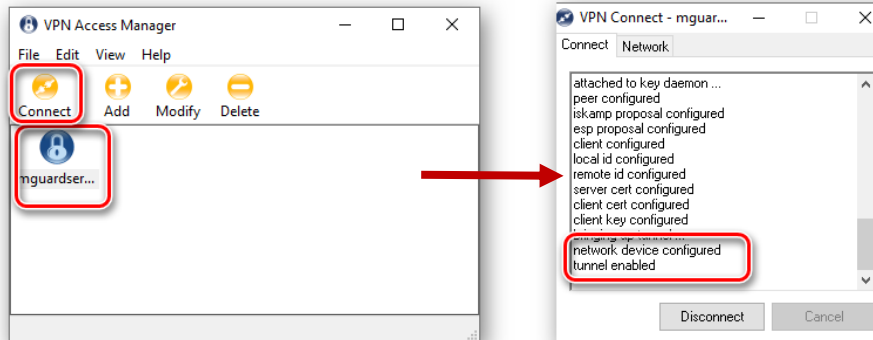
i) Clique **Save** para finalizar a configuração.

A configuração do ShrewSoft VPN Client está finalizada.

6. Inicializando e testando a conexão VPN

Para inicializar a conexão VPN entre o ShrewSoft e o mGuard, basta selecionar o ícone na tela do ShreSoft que representa a configuração criada anteriormente e clicar no botão Connect.

Na janela que abrirá, veremos o status da conexão. O status **"tunnel enabled"** significa que a conexão foi estabilizada com sucesso.



Selecionando, no menu da esquerda, a opção **IPsec VPN > IPsec Status** para monitorar o status da conexão no mGuard. Na figura abaixo é mostrado o status da conexão estabilizada.

