



Projeto Firewall 2015

Procedimento Instalação e Configuração VPN – Mac OS

Informações do Documento	
Cliente	SEGAD
Projeto/Atividade	Projeto Palo Alto 2015
Data de Realização	Agosto/2015

Cliente	SEGAD
Projeto/Atividade	Projeto Palo Alto 2015
Classificação	Confidencial

1. OBJETIVO	3
2. CENÁRIO	3
3. DEFINIÇÕES.....	3
3.1. TIPO DE VPN	3
3.2. ENDEREÇAMENTO IP	3
3.3. REQUISITO	3
4. PROCEDIMENTOS DE CONFIGURAÇÃO.....	5
4.1. DOWNLOAD DO GLOBALPROTECT.....	5
4.2. INSTALAÇÃO DO GLOBALPROTECT.....	6
4.3. CONFIGURAÇÃO DO GLOBALPROTECT.....	7
5. TESTES E TROUBLESHOOTING	9

Cliente	SEGAD
Projeto/Atividade	Projeto Palo Alto 2015
Classificação	Confidencial

1. OBJETIVO

Este documento tem como objetivo apresentar a documentação referente à Instalação e Configuração do Agente GlobalProtect necessário para viabilizar o acesso VPN (*Virtual Private Network*) à Sutic.

2. CENÁRIO

O Firewall central alocado nas dependências da Sutic possui todas as configurações necessárias para permitir o acesso VPN:

- O firewall central está com todos os túneis configurados, apenas aguardando as conexões remotas;

De modo geral, as únicas configurações a serem realizadas pelo usuário são:

- Realizar o Download e Instalação do Agente GlobalProtect;
- Configurar o Agente com os parâmetros: Endereço do Portal e Credenciais.

3. DEFINIÇÕES

3.1. TIPO DE VPN

A conectividade entre o site central (Sutic) e os clientes será via VPN do tipo client-to-site, GlobalProtect.

3.2. ENDEREÇAMENTO IP

O seguinte esquema de configuração IP foi definida para o projeto:

Objeto	Endereçamento IP	Observações
Rede local remota	10.78.xx.0/24	O “xx” é referente ao número alocado para os clientes de cada VPN baseado em sua Localidade;
Endereço IP do Portal do GlobalProtect	131.72.222.125	Para realizar o acesso ao GlobalProtect Portal

3.3. REQUISITO

O Agente possui suporte às seguintes Versões do MAC OS:

1. Apple MAC OS 10.6;
2. Apple MAC OS 10.7;
3. Apple MAC OS 10.8;
4. Apple MAC OS 10.9;
5. Apple MAC OS 10.10;

Cliente	SEGAD
Projeto/Atividade	Projeto Palo Alto 2015
Classificação	Confidencial

Cliente	SEGAD
Projeto/Atividade	Projeto Palo Alto 2015
Classificação	Confidencial

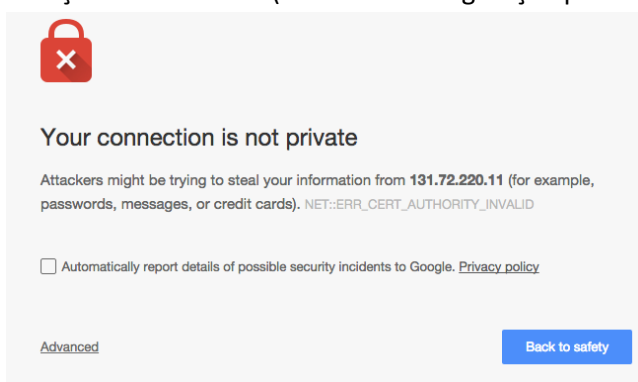
4. PROCEDIMENTOS DE CONFIGURAÇÃO

Para realizar o acesso VPN, é necessário realizar a configuração de um Agente (*Client-based*) que será responsável por permitir conexões VPN. Para isso, é necessário realizar o *download* do seu instalador.

4.1. DOWNLOAD DO GLOBALPROTECT

Para realizar o Download do GlobalProtect, siga os seguintes passos:

- 1) Via *browser*, acesse o endereço **https:// 131.72.222.125**;
- 2) Conforme imagem abaixo, um erro de Certificado irá aparecer. Adicione esse endereço (131.72.222.125) nas exceções do browser. (obs.: essa configuração pode variar de acordo como o navegador);



- 3) Na tela de autenticação, entre com suas credencias do domínio para realizar o Download;



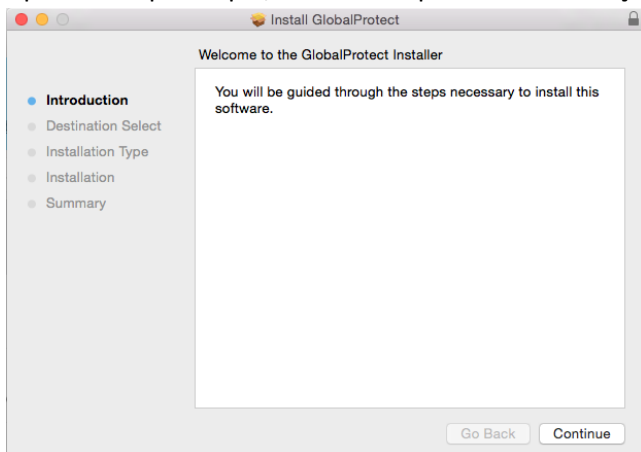
- 4) Selecione o instalador **Mac 32/64 bit GlobalProtect agent**;

Cliente	SEGAD
Projeto/Atividade	Projeto Palo Alto 2015
Classificação	Confidencial

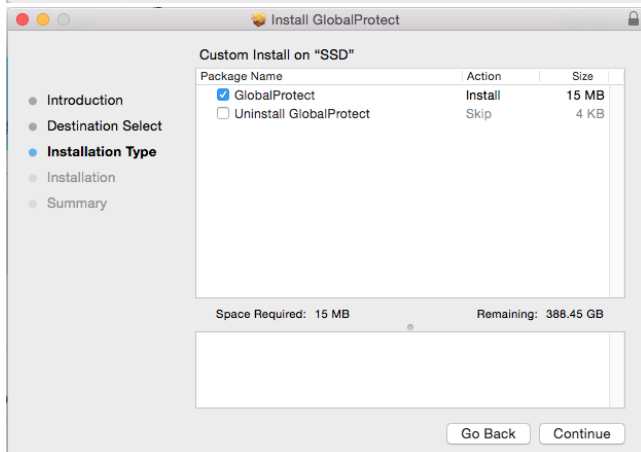


4.2. INSTALAÇÃO DO GLOBALPROTECT

- 1) Localize o Instalador GlobalProtect.pkg;
- 2) Após um duplo clique, avance nos passos de instalação, conforme imagens abaixo;

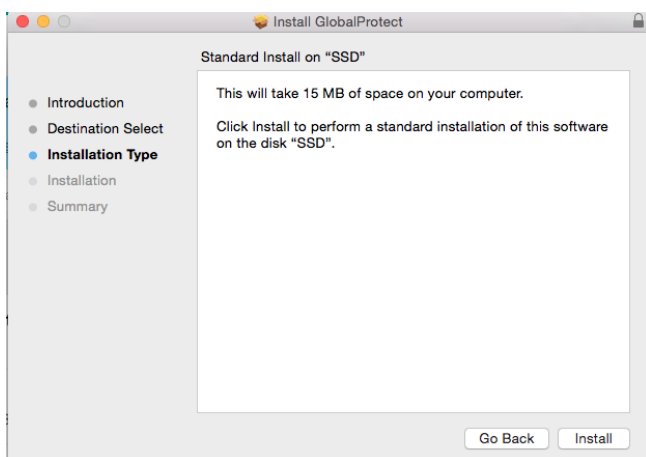


3)

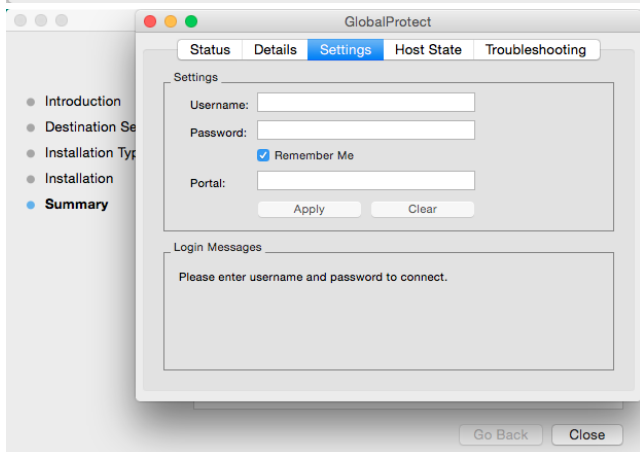


4)

Cliente	SEGAD
Projeto/Atividade	Projeto Palo Alto 2015
Classificação	Confidencial



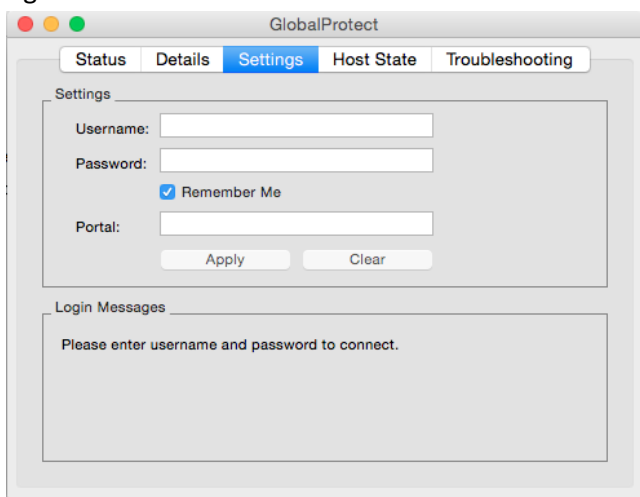
5)



6)

4.3. CONFIGURAÇÃO DO GLOBALPROTECT

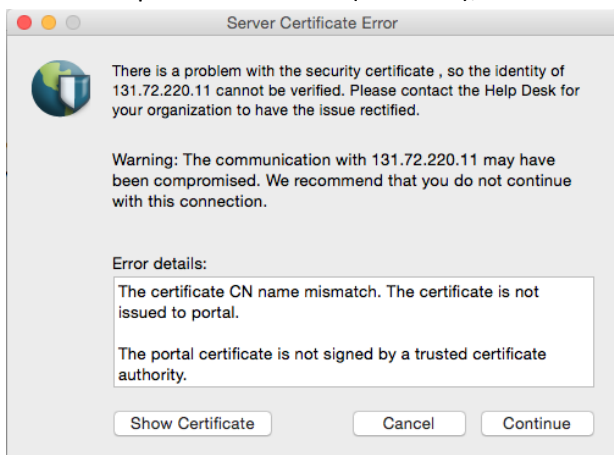
Após a instalação do GlobalProtect com sucesso, inicie o Programa GlobalProtect para realizar a configuração do Agente.



- 1) Em Settings;
- 2) Inserir os valores dos seguintes parâmetros:
 - a. Username: nome do usuário (o mesmo utilizado para realizar o download do agente.);
 - b. Password: senha pessoal;
 - c. Portal: **131.72.222.125**;

Cliente	SEGAD
Projeto/Atividade	Projeto Palo Alto 2015
Classificação	Confidencial

- 3) Clicar em Apply.
 - a. OBS: Quando clicar em Apply, o Agente tentará estabelecer uma conexão com o GlobalProtect Portal/Gateway. Um ícone no canto inferior direito irá aparecer com o status Connecting/Discovering Network}.
- 4) Ao tentar conectar ao GlobalProtect Portal, o agente irá apresentar um erro de Certificado, conforme imagem abaixo. Clique em Continuar (*continue*);



- 5) Se a conexão ocorrer tudo bem, em GlobalProtect > *status*, irá aparecer uma mensagem *Connected* e você estará apto a acessar serviços internos via VPN. Se não houver sucesso na conexão, ir à seção de Testes *Troubleshooting*;

Cliente	SEGAD
Projeto/Atividade	Projeto Palo Alto 2015
Classificação	Confidencial

5. TESTES E TROUBLESHOOTING

Após a configuração do GlobalProtect, o agente estará apto a conectar-se com o GlobalProtect Portal/Gateway configurados na SEDAD, permitindo acesso aos serviços internos via VPN. Para verificar essa conectividade, siga os passos:

- 1) Acesse o Terminal;
- 2) Digite “ifconfig” (sem aspas);
- 3) Observe se o IP da sua estação está na rede **10.78.0.0/24**;

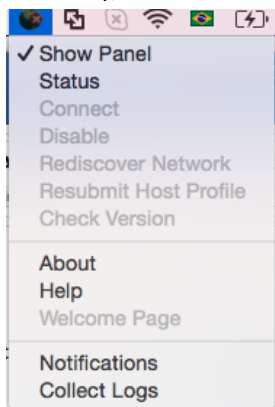
Para testa a conectividade:

- 1) Acesse o Terminal;
- 2) Digite “ping <endereço de algum servidor interno>” (sem aspas);
- 3) Se houver resposta, houve conectividade via VPN;

Caso não tenha sucesso nos passos acima, tente algum dos seguintes passos:

- 4) Verifique sua conexão com a Internet;

- 5) Tente conectar novamente (botão direito sobre o ícone do GlobalProtect no canto inferior direito > connect);



- a. Caso não esteja habilitado o botão *connect*, clique em Show Panel > Settings > Apply;
- 6) Verifique se os parâmetros estão corretos:
 - a. Username: usuário do domínio para acesso VPN;
 - b. Password: senha pessoal;
 - c. Portal Address: 131.72.222.235;
- 7) Quando o erro de certificado aparecer, clique em Continuar;
- 8) Caso não consiga estabelecer a comunicação VPN, entre em contato com a equipe técnica da Sutic.