



## Projeto Firewall 2015

### Procedimento Instalação e Configuração VPN – Android

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

<b>1. OBJETIVO .....</b>	<b>3</b>
<b>2. CENÁRIO .....</b>	<b>3</b>
<b>3. DEFINIÇÕES.....</b>	<b>3</b>
3.1. TIPO DE VPN .....	3
3.2. ENDEREÇAMENTO IP .....	3
3.3. REQUISITO .....	3
<b>4. PROCEDIMENTOS DE CONFIGURAÇÃO.....</b>	<b>4</b>
4.1. CONFIGURAÇÃO DO CLIENT IPSEC .....	4
<b>5. TROUBLESHOOTING.....</b>	<b>5</b>

Cliente	SEGAD
Projeto/Atividade	Projeto Palo Alto 2015
Classificação	Confidencial

## 1. OBJETIVO

Este documento tem como objetivo apresentar a documentação referente à configuração necessária para conexão necessária 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, a única configuração a ser realizada pelo usuário é:

- Configuração do Android IPSec Client;

## 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, utilizando o Agente do Android IPSec.

### 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 ao iOS que possui:

1. Android Client IPSec;

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 a configuração do Client IPsec do Android.

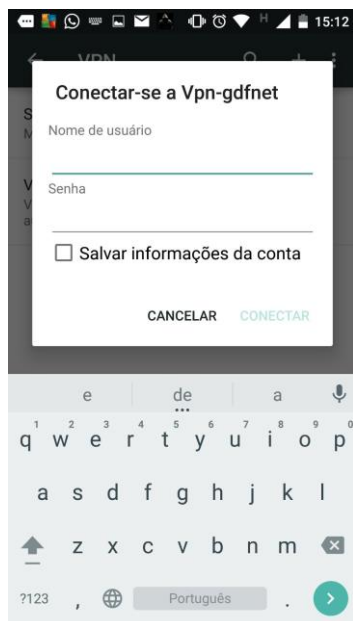
### 4.1. CONFIGURAÇÃO DO CLIENT IPSEC

- 1) Em Configurações > ... > VPN, adicione uma nova configuração de VPN;
  - a. Essa etapa pode variar de acordo com a versão do Android;
- 2) Escolha o tipo IPsec Xauth PSK;
- 3) Insira os seguintes parâmetros:
  - a. Nome: defina um nome para a VPN;
  - b. Tipo: IPsec Xauth PSK;
  - c. Endereço do Servidor: **131.72.222.235;**
  - d. Identificador IPsec: **vpngdfnet;**
  - e. Senha pré-compartilhada IPsec: **cetic;**




- 4) Salve as configurações e tente conectar à VPN;
- 5) Quando for requisitado, insira suas credenciais e clique em Conectar;

Cliente	SEGAD
Projeto/Atividade	Projeto Palo Alto 2015
Classificação	Confidencial



6) Caso seja apresentado um erro de Certificado, clique em Continuar;

## 5. TROUBLESHOOTING

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

- 1) Verifique sua conexão com a Internet (3G/4G ou WiFi);
- 2) Tente conectar novamente;
- 3) Verifique se os parâmetros estão corretos:
  - a. Tipo: IPSec Xauth PSK;
  - b. Endereço do Servidor: **131.72.222.235**;
  - c. Identificador IPSec: **vpngdfnet**;
  - d. Senha pré-compartilhada IPSec: **cetic**;
  - e. Usuário e Senha;
- 4) Quando o erro de certificado aparecer, clique em Continuar;
- 5) Caso não consiga estabelecer a comunicação VPN, entre em contato com a equipe técnica da Sutic.