



GUIA DE CONFIGURAÇÃO

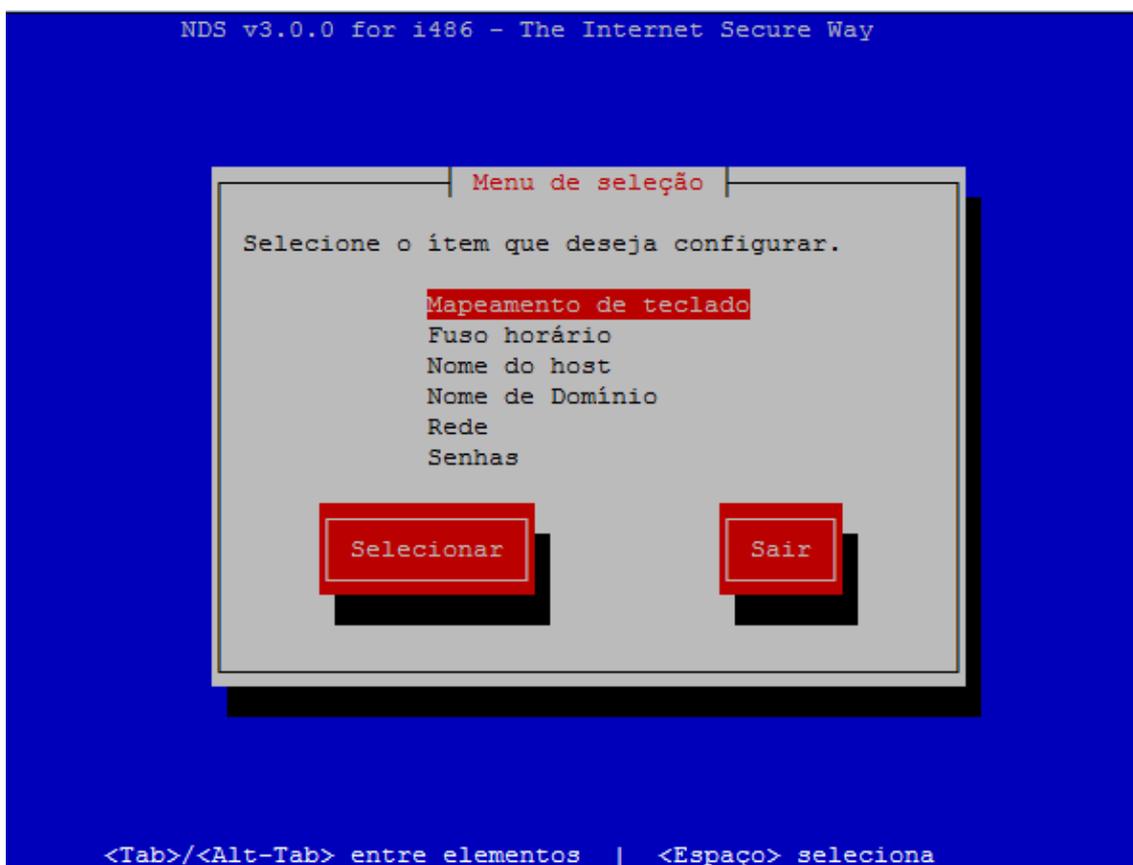
AUTENTICAÇÃO TRANSPARENTE DO
PROXY COM O ACTIVE DIRECTORY

AUTENTICAÇÃO TRANSPARENTE DO PROXY COM ACTIVE DIRECTORY

1- Preparando o Netdeep Secure

O DNS primário do firewall precisa ser o IP do servidor do Active Directory. Para isso conecte no firewall por ssh ou no console com o usuário **root** e logo em seguida digite **setup** e pressione a tecla **ENTER**.

Irá exibir uma tela azul, escolha a opção **Rede** e pressione **ENTER**



Agora selecione a opção **Configurações de DNS e Gateway** e pressione **ENTER**

Menu de configuração de rede

Selecione o item que deseja configurar.

Tipo da configuração RED
Atribuições de drivers e placas
Configuração do ISDN.
Configurações de endereço
Configurações de DNS e Gateway
Nome do host

Selecionar

Voltar

<Tab>/<Alt-Tab> entre elementos | <Espaço> seleciona

Apague o que estiver digitado no DNS primário e digite o IP de seu servidor Active Directory.
Obs.: no nosso exemplo o IP do AD é 192.168.1.74

Configurações de DNS e Gateway

Forneça as informações de DNS e gateway. Estas configurações apenas serão usadas com IP Estático (e DHCP se o DNS estiver configurado) na interface RED.

DNS Primário	192.168.1.74
DNS secundário	8.8.4.4
Gateway Padrão	192.168.1.1

Ok

Voltar

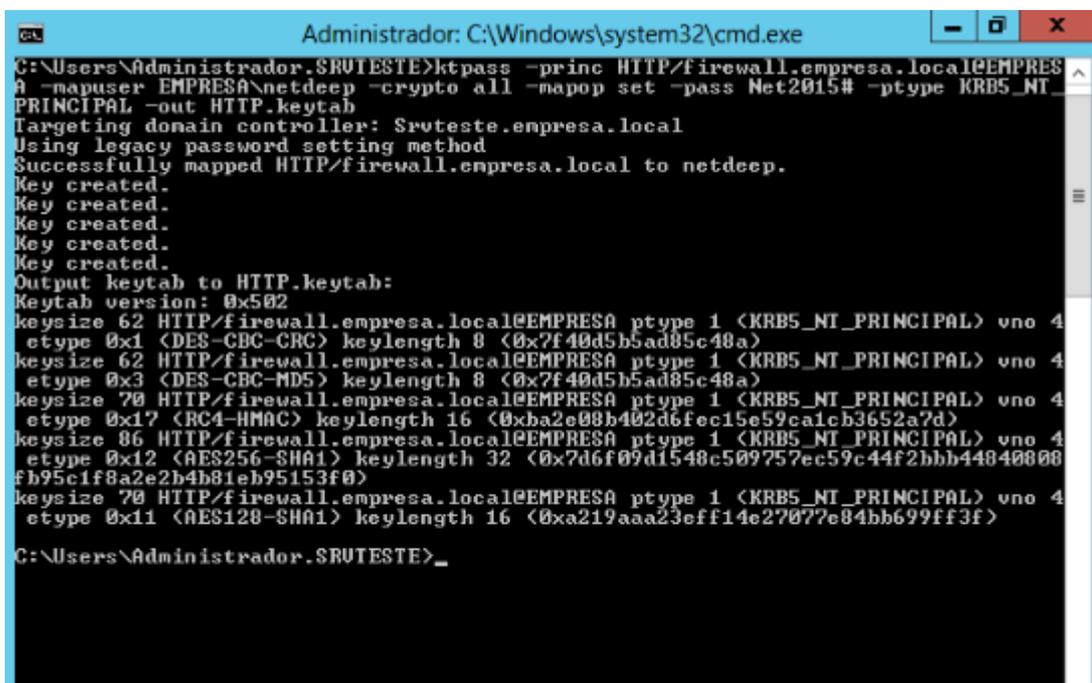
<Tab>/<Alt-Tab> entre elementos | <Espaço> seleciona


```
ktpass -princ HTTP/<fqdn do firewall>@<DOMINIO> -mapuser
<DOMINIO\usuario> -crypto all -mapop set -pass <Senha do usuario de
bind> -ptype KRB5_NT_PRINCIPAL -out HTTP.keytab
```

- **fqdn do firewall:** é o DNS que configuramos para o firewall + o domínio (**firewall.empresa.local**)
- **DOMINIO:** é seu domínio em letra MAIÚSCULA (**EMPRESA**)
- **usuário:** é o usuário criado anteriormente (**netdeep**)
- **Senha do usuário de bind:** é a senha do usuário(netdeep) que foi criada, no meu caso **Net2015#**

Feita a alteração, o comando ficaria da seguinte maneira:

```
ktpass -princ HTTP/firewall.empresa.local@EMPRESA -mapuser EMPRESA\netdeep -crypto all -mapop
set -pass Net2015# -ptype KRB5_NT_PRINCIPAL -out HTTP.keytab
```

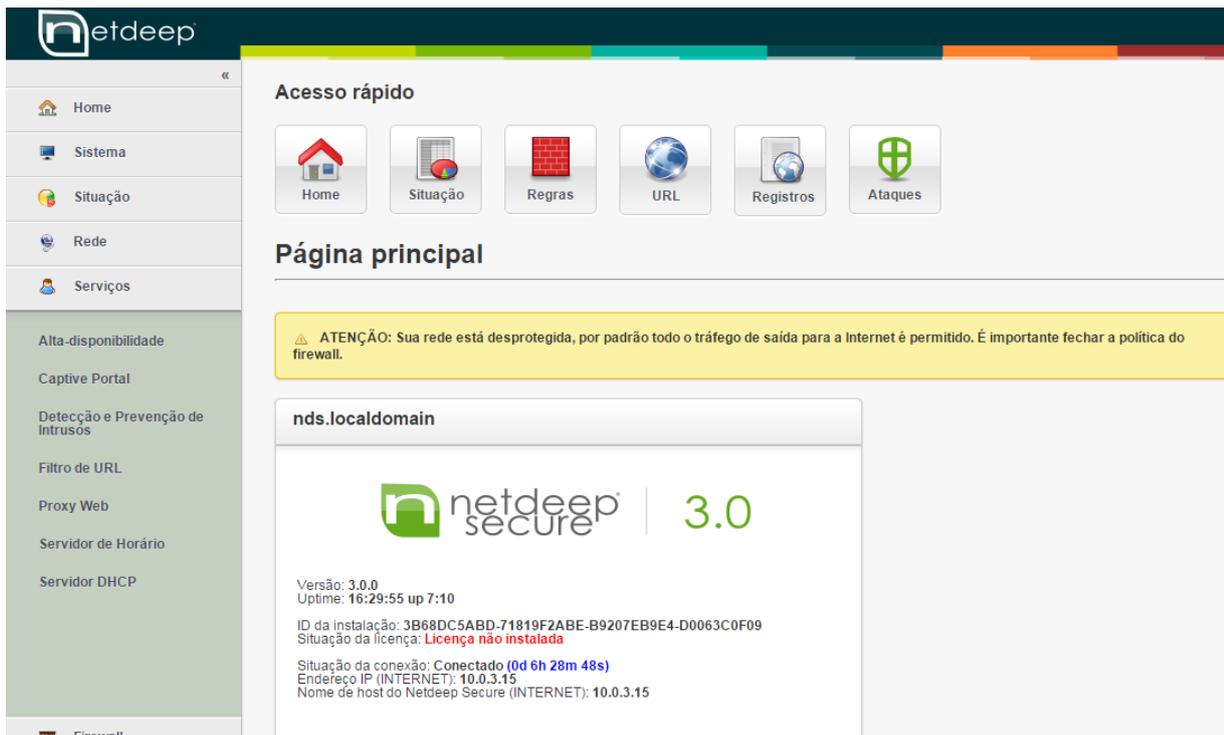


```
Administrador: C:\Windows\system32\cmd.exe
C:\Users\Administrador.SRVTESTE>ktpass -princ HTTP/firewall.empresa.local@EMPRES
A -mapuser EMPRESA\netdeep -crypto all -mapop set -pass Net2015# -ptype KRB5_NT
PRINCIPAL -out HTTP.keytab
Targeting domain controller: Srvteste.empresa.local
Using legacy password setting method
Successfully mapped HTTP/firewall.empresa.local to netdeep.
Key created.
Key created.
Key created.
Key created.
Key created.
Output keytab to HTTP.keytab:
Keytab version: 0x502
keysize 62 HTTP/firewall.empresa.local@EMPRESA ptype 1 <KRB5_NT_PRINCIPAL> vno 4
 etype 0x1 <DES-CBC-CRC> keylength 8 <0x7f40d5b5ad85c48a>
keysize 62 HTTP/firewall.empresa.local@EMPRESA ptype 1 <KRB5_NT_PRINCIPAL> vno 4
 etype 0x3 <DES-CBC-MD5> keylength 8 <0x7f40d5b5ad85c48a>
keysize 70 HTTP/firewall.empresa.local@EMPRESA ptype 1 <KRB5_NT_PRINCIPAL> vno 4
 etype 0x17 <RC4-HMAC> keylength 16 <0xba2e00b402d6fec15e59ca1cb3652a7d>
keysize 86 HTTP/firewall.empresa.local@EMPRESA ptype 1 <KRB5_NT_PRINCIPAL> vno 4
 etype 0x12 <AES256-SHA1> keylength 32 <0x7d6f09d1548c509757ec59c44f2bbb44840000
fb95c1f8a2e2b4b81eb95153f0>
keysize 70 HTTP/firewall.empresa.local@EMPRESA ptype 1 <KRB5_NT_PRINCIPAL> vno 4
 etype 0x11 <AES128-SHA1> keylength 16 <0xa219aaa23eff14e27077e84bb699ff3f>
C:\Users\Administrador.SRVTESTE>_
```

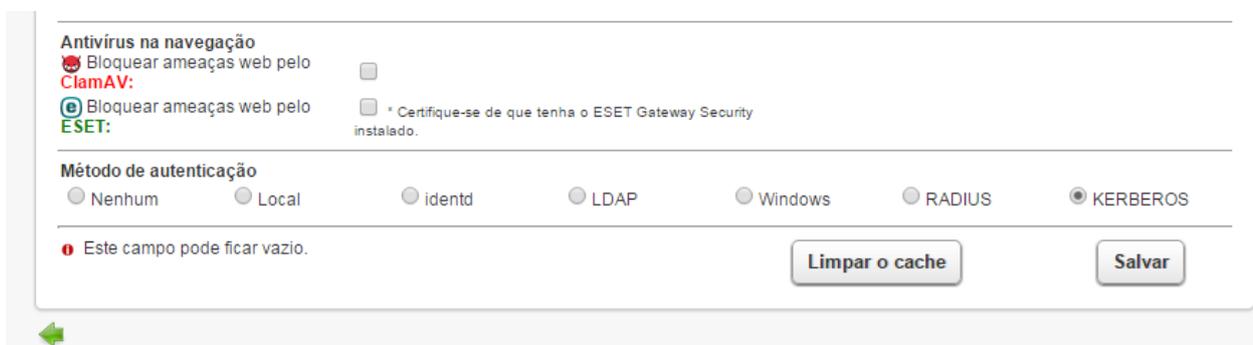
O arquivo **HTTP.keytab** será criado no diretório onde o comando foi executado. No exemplo acima o arquivo foi criado em **C:\Users\Administrador.SRVTESTE**

3- Configurando o Netdeep Secure

Abra a interface gráfica do firewall utilizando um navegador de internet. Em seguida, no menu esquerdo, clique em **Serviços** e no menu que é exibido escolha a opção **Proxy Web**.



Após o carregamento da pagina, desça a barra de rolagem até o final da pagina. Em “**Método de autenticação**” selecione a opção “**KERBEROS**” e clique em **Salvar**.



Irá carregar novamente a tela exibindo a configuração do Kerberos.

Para visualizar as configurações desça novamente a barra de rolagem até o final da página e preencha os campos mencionados abaixo para realizar as configurações de autenticação.

Domínio do Active Directory: você deve colocar o seu domínio (Exemplo: empresa.local)

FQDN do servidor de AD: é o nome do servidor do AD + domínio (Exemplo: srvteste.empresa.local)

FQDN do firewall do domínio: é o nome do DNS configurado anteriormente no AD para o firewall + domínio (Exemplo: firewall.empresa.local)

Usuário para bind do AD (usuário@dominio): é o nome de usuário criado anteriormente + domínio (Exemplo: netdeep@empresa.local)

Senha: é a senha criada para o usuário.

Arquivo Keytab: é o arquivo que foi gerado através do comando executado no prompt do AD.

Método de autenticação

Nenhum
 Local
 identd
 LDAP
 Windows
 RADIUS
 KERBEROS

Configuração global de autenticação

Número de processos de autenticação:

Cache de autenticação TTL (em minutos):

Limite de endereço IP por usuário:

Cache Usuário/IP TTL (em minutos):

Requer autenticação para fonte de endereços irrestrita:

Campo de autenticação:
 Domínios sem autenticação (um por linha):

Configuração do Kerberos

Domínio do Active Directory:
 Criptografia AES: Não Sim

FQDN do servidor de AD:
 FQDN do firewall no domínio:

Usuário para bind no AD (usuario@dominio):
 Senha:

DN do grupo de acesso:

Arquivo Keytab: Nenhum arquivo selecionado

* O arquivo de Keytab deve ser criado com o seguinte comando no prompt do AD:
 ktpass -princ HTTP/<fqdn do firewall>@<DOMINIO> -mapuser <DOMINIO/usuario> -crypto all -mapop set -pass <Senha do usuario de bind> -ptype KRB5_NT_PRINCIPAL -out HTTP

Keytab:
 Keytab name: FILE:/var/netdeep/proxy/HTTP.keytab
 KVNO Principal

3 HTTP/firewall.empresa.local@EMPRESA
 3 HTTP/firewall.empresa.local@EMPRESA
 3 HTTP/firewall.empresa.local@EMPRESA
 3 HTTP/firewall.empresa.local@EMPRESA
 3 HTTP/firewall.empresa.local@EMPRESA

Este campo pode ficar vazio.

Após o preenchimento de todos os campos e importado o arquivo Keytab, clique em **Salvar**.

IMPORTANTE: nas configurações de Proxy de cada estação que irá ser autenticada de forma transparente, o endereço do servidor Proxy de cada estação deve ser o DNS que foi criado + domínio, a porta é a que esta configurada no firewall.

No nosso exemplo o endereço seria: **firewall.empresa.local**

Configurações da Rede Local (LAN)

Configuração automática

A configuração automática poderá substituir as configurações manuais. Para usar as configurações manuais, desabilite a configuração automática.

Detectar automaticamente as configurações
 Usar script de configuração automática

Endereço:

Servidor proxy

Usar um servidor proxy para a rede local (estas configurações não se aplicam a conexões discadas ou VPN).

Endereço: Porta:

Não usar servidor proxy para endereços locais

4- Para saber mais

<http://www.netdeep.com.br/secure/>