

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

NDS	v3.0.0 for i486 - The Internet Secure Way
	Menu de seleção
	Selecione o ítem que deseja configurar.
	Mapeamento de teclado
	Fuso horário
	Nome do host
	Nome de Domínio
	Rede
	Senhas
	Selecionar
<tab>/<a< td=""><td>Alt-Tab> entre elementos <espaço> seleciona</espaço></td></a<></tab>	Alt-Tab> entre elementos <espaço> seleciona</espaço>

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

NDS v3.0.0 for i486 - The Internet Secure Way
Menu de configuração de rede
Selecione o ítem que deseja configurar.
Tipo da configuração RED Atribuições de drivers e placas Configuração do ISDN. Configurações de endereço <mark>Configurações de DNS e Gateway</mark> Nome do host
Selecionar
<tab>/<alt-tab> entre elementos <espaço> seleciona</espaço></alt-tab></tab>

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**



Depois escolha a opção **OK.** Irá voltar para tela de "**Menu de configuração de rede**", escolha a opção **Voltar**, irá exibir uma tela "**Reconfigurando as redes...**" aguarde até que seja realizada a configuração e em seguida escolha a opção **Sair.**

2- Preparando o Active Directory

Utilizando o snap in **"Usuários e computadores do Active Directory**" crie um usuário comum (por exemplo: na chave**<domínio> , Users**, crie o usuário **netdeep**) para conexão com o Active Directory. Ele não precisa estar em nenhum grupo especial.

Em "Gerenciador DNS" navegue até Zonas de pesquisa direta e clique com o botão direito em cima do seu domínio (no meu exemplo empresa.local) e escolha a opção Novo Host(A ou AAAA)...

Em "Host" digite firewall e em "Endereço IP" digite o endereço IP da GREEN do firewall (como no exemplo abaixo) em seguida clique em OK.

å Gerenciador DNS							٥	x
Arquivo Ação Exibir Ajuda								
🗢 🔶 🙍 🗙 🖾 😹 📓 🗐 🗐								
 DNS SRVTESTE Image: Constant of the second state of the second stat	Nome msdcssites Propriedad Host (A) Segurança Host (usa domínio pai se deixado en firewall Nome de domínio totalmente qualifi firewall.empresa local Endereço IP: 192.168.1.42Atualizar o registro de ponteiro a	Tipo des de firewall m branco): cado (FQDN): ssociado (PTR) DK Cancelar	Pados	e.empresa.loca presa.local. 4 2	Carimbo de data/h static 26/05/2015 10:00:0 static	D		

Agora é necessário que você gere o arquivo Keytab que iremos utilizar na configuração do Netdeep Secure.

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
```

- 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



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.**

«	Acesso rápido
🕎 Sistema	
🕞 Situação	Home Situação Regras URL Registros Ataques
👳 Rede	Página principal
🚨 Serviços	
Alta-disponibilidade	🔊 ATENÇÃO: Sua rede está desprotegida, por padrão todo o tráfego de saída para a Internet é permitido. É importante fechar a política do firewall.
Captive Portal	
Detecção e Prevenção de Intrusos	nds.localdomain
Filtro de URL	
Proxy Web	
Servidor de Horário	
Servidor DHCP	Versão: 3.0.0 Uptime: 16:29:55 up 7:10
	ID da instalação: 3B68DC5ABD-71819F2ABE-B9207EB9E4-D0063C0F09 Situação da licença: Licença não instalada
	Situação da conexão: Conectado (0d 6h 28m 48s) Endereço IP (INTERNET): 10.0.3.15 Nome de host do Netdeep Secure (INTERNET): 10.0.3.15
Firewall	

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.**

• Este campo pode ficar vazio.			Limpa	Salvar		
Método de autenti O Nenhum	cação O Local	identd	LDAP	Windows	RADIUS	KERBEROS
Bloquear amea ClamAV: Bloquear amea Bloquear amea ESET:	ças web pelo ças web pelo	* Certifique-se de qu instalado.	e tenha o ESET Gatewa	y Security		

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 autenti	icação							
Nenhum	Local	identd	LDAP	Windows	RADIUS	KERBEROS		
Configuração glol	bal de autenticaç	ão						
Número de proces autenticação:	sos de	5	Campo de autenticação: 0					
Cache de autentic minutos):	ação TTL (em	60		Domínios sem autentica	ação (um por linha): ()		
Limite de endereço D	o IP por usuário:							
Cache Usuário/IP	TTL (em minutos)	: 0						
Requer autenticaç endereços irrestrit	ão para fonte de a:							
						<u>//</u>		
Configuração do I	Kerberos		1					
Domínio do Active	Directory:	empresa.local		Criptografia	a AES:	Não 🔍 Sim 🖲		
QDN do servidor	de AD:	srvteste.empresa.loc	FQDN do firewall no dominio:		firewall.empresa.lo			
Usuário para bind (usuario@dominio	no AD):	netdeep@empresa.lo		Senha:		••••••		
DN do grupo de ac	cesso:0							
Arquivo Keytab:		Escolher arquivo Ne	enhum arqui∨o	selecionado				
O arquivo de Keytat ktpass -princ HTTP/ <f< td=""><td>b deve ser criado cor qdn do firewall>@<d< td=""><td>n o seguinte comando no pro OMINIO> -mapuser <dominio< td=""><td>mpt do AD: O∖usuario> -crypt</td><td>o all -mapop set -pass <senh< td=""><td>a do usuario de bind> -p</td><td>type KRB5_NT_PRINCIPAL ⊣</td></senh<></td></dominio<></td></d<></td></f<>	b deve ser criado cor qdn do firewall>@ <d< td=""><td>n o seguinte comando no pro OMINIO> -mapuser <dominio< td=""><td>mpt do AD: O∖usuario> -crypt</td><td>o all -mapop set -pass <senh< td=""><td>a do usuario de bind> -p</td><td>type KRB5_NT_PRINCIPAL ⊣</td></senh<></td></dominio<></td></d<>	n o seguinte comando no pro OMINIO> -mapuser <dominio< td=""><td>mpt do AD: O∖usuario> -crypt</td><td>o all -mapop set -pass <senh< td=""><td>a do usuario de bind> -p</td><td>type KRB5_NT_PRINCIPAL ⊣</td></senh<></td></dominio<>	mpt do AD: O∖usuario> -crypt	o all -mapop set -pass <senh< td=""><td>a do usuario de bind> -p</td><td>type KRB5_NT_PRINCIPAL ⊣</td></senh<>	a do usuario de bind> -p	type KRB5_NT_PRINCIPAL ⊣		
Keytab: Keytab name: FILE KVNO Principal	E:/var/netdeep/pro	xy/HTTP.keytab						
3 HTTP/firewall.e 3 HTTP/firewall.e 3 HTTP/firewall.e 3 HTTP/firewall.e 3 HTTP/firewall.e	empresa.local@El empresa.local@El empresa.local@El empresa.local@El empresa.local@El	MPRESA MPRESA MPRESA MPRESA MPRESA						
Este campo poo	de ficar vazio.			Limpa	r o cache	Salvar		

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

<u>IMPORTANTE</u>: nas configurações de Proxy de cada estação que irá ser autenticada de forma transparente, o endereço do servidor Proxy devera 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 (L	AN)			8				
Configuração au	tomática								
A configuração a manuais. Para u configuração au	A configuração automática poderá substituir as configurações manuais. Para usar as configurações manuais, desabilite a configuração automática.								
Detectar aut	omaticamente as co	onfiguraçi	ões						
🔲 Usar script de	e configuração auto	omática							
Endereço									
Servidor proxy									
Usar um serv se aplicam a o	idor proxy para a r conexões discadas	ede local ou VPN).	(estas co	nfigurações n	ão				
Endereço:	firewall.empresa	Porta:	3128	Avançada	is				
☑ Não usar servidor proxy para endereços locais									
			ОК	Cancel	ar				

4- Para saber mais

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