



Guia de Referência Rápida

Configuração de VPN entre mGuard e ShrewSoft app



Índice

1.	Introdução	3
2.	Cenário utilizado como exemplo neste quia	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:

00100 0011010010000	o oogannoo n'o para oota ooringarayao.
- 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 ShrewS	Soft : 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
 Certification

0

- 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

0

- 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 <u>https://192.168.1.1</u> 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.

mGuard (mguard)	× +	- ° X
$\leftarrow \rightarrow$ C \textcircled{A} V	lão seguro https://192.168.1.1/index.cgi	$A^{\mathbb{N}}$ $\mathcal{L}_{\mathbb{D}}$ $\mathcal{L}_{\mathbb{D}}$ $\mathcal{L}_{\mathbb{D}}$ Convidado (2) …
	WARNING: THE ROOT PASS Logged in as admin with role a	MORD IS NOT CONFIGURED! dmin from 192.168.1.221. Authenticated by login.
8.8.6.default Wednesday, October 19 2022 15:33:54		Ŏ 00:29:53
Management	Management » System Settings	
System Settings Web Settings	Host Time and Date Shell Access	E-Mail
Licensing Update	System	0
Configuration Profiles SNMP	State of the power supply 1	Power supply 1 working
Central Management	State of the power supply 2	Power supply 2 out of order
Service I/O	Suctom tomporaturo	Min: 0 90 Current: Max: 60 90 Temporature 0K
Restart	System temperature	
Authentication	System use notification	The usage of this mGuard security appliance is reserved to authorized staff only. Any intrusion and its attempt w
Network Security		
IPsec VPN	System DNS Hostname	
OpenVPN Client	Hostname mode	User defined (from field below)
Logging	Hostname	mquard
Support		
	Domain search path	example.local
	SNMP Information	
	System name	•
Copyright © 2001-2022 PHOENIX CONT/	ACT Cyber Security GmbH and others Legal Notice Trademarks	& Patents mGuard Documentation

4.2 Configuração dos endereços IPs das portas LAN e WAN

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

- a) Acesse, no menu da esquerda, a opção Network > Interfaces.
- b) 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.

🔲 🚺 mGuard (mguard)	× +		= - @ ×
\leftarrow \rightarrow C a \checkmark	Não seguro https://192.168.1.1/index.cgi		A ^N t _o t Convidado (2) ···
	WARNING: THE ROOT PASS Logged in as admin with role a	WORD IS NOT CONFIGURED! dmin from 192.168.1.221. Authenticated by login.	D ¢ U
8.8.6.default Wednesday, October 19 2022 15:47:17			₫ 00:23:25
Management	Network » Interfaces		
System Settings Web Settings	General External Internal DMZ	Secondary External	
Licensing Update	Network Status		0
Configuration Profiles	External IP address	10.0.0.152	
Central Management	Current default route	10.0.0.253	
Restart	Used DNS servers	DNS root servers	
Network	Network Mode		
Interfaces		1	
Mobile Network	Network mode	Router	
Serial Line Ethernet	Router mode	Static	-
NAT		I.	
DNS			
DHCP			
Proxy Settings			
Dynamic Routing			
GRE Tunnel			
Authentication	*		
Copyright © 2001-2022 PHOENIX C	NNTACT Cyber Security GmbH and others Legal Notice Trademark	s & Patents	mGuard Documentation





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).

letwork » Interfaces					
General Exter	nal Internal DMZ	Secondary External			
External Networks			_	?	
Seq. 🕂	IP address	Netmask	Use VLAN VLAN ID		
1	192.168.3.3	255.255.255.0	1		
Additional Externa	l Routes		la la		
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.

nternal Networ	ks			Ċ
Seq. 🕂	IP address	Netmask	Use VLAN VLAN ID	
1	192.168.0.1	255.255.255.0	1	

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 CONFIGUREDI Logged in as admin with role admin from 192.168.0.221. Authenticated by login. 0 00:29:01					© 00:29:08
Management	Network » Interfaces					
Network	Coursel Costan	al Tubunal Dur	Consultant External			
Interfaces	General Extern	Internal DMZ	Secondary External			
Mobile Network	Internal Networks					0
Serial Line						<u> </u>
Ethernet	Seq. (+)	IP address	Netmask	Use VLAN	VLAN ID	
NAT	_					
DNS	1	192.168.0.1	255.255.255.0		1	
DHCP						
Proxy Settings	Additional Internal	Routes				
Dynamic Routing						
GRE Tunnel	Seq. (+)		Network	Gi	ateway	
Authentication						

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 (<u>https://192.168.0.1</u>).

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 valido 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:

- a) Acesse, no menu da esquerda, a opção Network > DNS. Selecione a aba DynDNS.
- b) 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.
- c) Clique no ícone superior no formato de um disquete, para salvar a configuração.

🔲 😰 mGuard (mguard)	× +		- 0 X
\leftarrow \rightarrow C \bigcirc	Não seguro https://192.168.0.1/index.cgi		A ^N tà t≌ Convidado 🙆 …
	WARNING: THE ROOT PASS Logged in as admin with role a	WORD IS NOT CONFIGURED! dmin from 192.168.0.221. Authenticated by login.	🖬 ¢ U
8.8.6.default Tuesday, November 8 2022 09:40:04			₫ 00:29:52
Management	Network » DNS		
Network Interfaces	DNS server DynDNS		
Mobile Network	DynDNS		0
Serial Line	- ,		Ű
Ethernet	Register the mGuard at a DynDNS service		
DNS	State of the dyndns registration	DynDNS service disabled	
DHCP			
Proxy Settings	Status message		
Dynamic Routing	Refresh interval	0:07:00	seconds (hh:mm:ss)
GRE Tunnel			
Authentication	DynDNS provider	No-ip.com	
IPsec VPN	DynDNS login	gmail.com	
OpenVPN Client	DynDNS password	@	
QoS	-,,		
Logging	DynDNS hostname	mguardserver.ddns.net	
Support		10	
Copyright © 2001-2022 PHOENIX CO	NTACT Cyber Security GmbH and others Legal Notice Trademarks	& Patents	mGuard Documentation

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

DNS server DynDNS					
DynDNS		0			
Register the mGuard at a DynDNS service					
State of the dyndns registration	Successfully updated DynDNS IP				
Status message	0: No IP# change detected, still at 186.				
Refresh interval	0:07:00	seconds (hh:mm:ss)			
DynDNS provider	No-ip.com	-			
DynDNS login	0gmail.com				
DynDNS password					
DynDNS hostname	mguardserver.ddns.net				

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 Forward	ing					
Protocol	From IP	From port	Incoming on IP	Incoming on port	Redirect to IP	Redirect to port
UDP 🗸	0.0.0/0	any	- %extern	500	192.168.3.3	500
UDP -	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

mGuard (mguard)	x +	- 0 ×
\leftarrow $ ightarrow$ C \bigtriangleup Λ	Não seguro https://192.168.0.1/index.cgi A [®] S ₀ S [*] C [*] (Convidado 🕘 …
8.8.6.default	WARNING: THE ROOT PASSWORD IS NOT CONFIGURED! Logged in as admin with role admin from 192.168.0.221. Authenticated by login.	D \$ U
Friday, November 4 2022 15:41:41		₫ 00:26:28
Management	Authentication » Certificates	
Network Authentication	Certificate Settings Machine Certificates CA Certificates Remote Certificates CRL	
Administrative Users	Machine Certificates	0
Firewall Users RADIUS Certificates	Seq. 🕞 Short name Certificate details	
Network Security	1 🕂 T	
OpenVPN Client		
QoS		
Support		
	-	
Copyright © 2001-2022 PHOENIX CO	NTACT Cyber Security GmbH and others Legal Notice Trademarks & Patents	mGuard Documentation

- 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

🔲 🕑 mGuard (mguard)	× +	– o ×
\leftarrow \rightarrow C \textcircled{A}	ão seguro https://192.168.0.1/index.cgi	$\mathbb{A}^{\mathbb{N}}$ $\mathfrak{C}_{\mathfrak{D}}$ $\mathfrak{C}_{\mathfrak{T}}$ Convidado 🙆 …
8.8.6.default	WARNING: THE ROOT PASSWORD IS NOT CON Logged in as admin with role admin from 192.168.0	IGUREDI 221. Authenticated by login.
Friday, November 4 2022 15:51:31		₫ 00:29:00
Management	Authentication » Certificates	
Network	Cortificato Sottings Machina Cortificatos	Romoto Cartificator CRI
Authentication	Certificate Settings Machine Certificates	
Administrative Users	Trusted CA Certificates	\bigcirc
Firewall Users		
RADIUS	Seq. (+) Short name	Certificate details
Certificates		
Network Security	1 (+)	🗅 🏦 Upload
IPsec VPN		
OpenVPN Client		
QoS		
Logging		
Support		

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.

🔲 💽 mGuard (mguard)							
\leftarrow \rightarrow C \textcircled{a} A	Vão seguro https://192.1	68.0.1/index.cgi				A* t₀ t≞ (Convidado 🕘 …
		WARNING: THE ROOT PASSU Logged in as admin with role ad	VORD IS NOT CON Imin from 192.168.0	FIGURED! .221. Authenticated by login.			D ¢ U
Friday, November 4 2022 16:02:13							₫ 00:29:52
Management	IPsec VPN » Connection	s					
Network Authentication	Connections						
Network Security	License Status						0
Global		VPN license counter	0				
L2TP over IPsec		OpenVPN license counter	0				
IPsec Status OpenVPN Client	Connections						
QoS	Seq. 🕕	Initial mode	State	ISAKMP SA	IPsec SA	Name	
Logging Support	1 🕂 🗐	Started -				(unnamed)	
	·						

- 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.

🔲 🕑 mGuard (mguard)	× +				- 0 ×
\leftarrow \rightarrow C Q \blacktriangle	Não seguro https://192.16	58.0.1/index.cgi		A" Q (2)	£≞ Convidado @ …₀
8.8.6.default		WARNING: THE ROOT PASSV Logged in as admin with role ad	VORD IS NOT CONFIGURED! min from 192.168.0.221. Authenticated by login.		D \$\$ \$U\$
Friday, November 4 2022 16:15:53					₫ 00:24:50
Management IP	Psec VPN » Connections » (u	nnamed)			
Network	General Authenticatio	on Firewall IKE Opt	ions		
Authentication Network Security	Options				? ^
IPsec VPN Global	A descript	ive name for the connection	ShrewSoft_VPN		
Connections		Initial mode	Started		•
IPsec Status OpenVPN Client OnS	Address of the remote site' hostname, or '%any' fo clie	s VPN gateway (IP address, or any IP, multiple clients or ents behind a NAT gateway)	%any		
Logging	Interface to us	e for gateway setting %any	External		•
Support		Connection startup	Wait		•
		Controlling service input	None		•
		Deactivation timeout	0		seconds (hh:mm:ss)
	Tok	ken for text message trigger			
	Encape	sulate the VPN traffic in TCP	No		•
	Mode Configuration				
		Mode configuration	Off		•
Copyright © 2001-2022 PHOENIX CONTAC	T Cyber Security GmbH and others	Legal Notice Trademarks & Patent	5		mGuard Documentation

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.

Mode Configurat	ion				
		Mode configuration Off			•
Transport and Tu	unnel Settings				
iment	Туре	Local	Local NAT	Remote	Remote NAT
	Tunnel		No NAT 👻	192.168.4.1/32	No NAT -
4					۰.

- 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.

🔲 🕑 mGuard (mguard)	× +	- 0 X
\leftarrow \rightarrow C \otimes	Não seguro https://192.168.0.1/index.cgi	AN Q 56 51 Convidado 🙆 🗤
	WARNING: THE ROOT PASSWORD IS NOT CONF Logged in as admin with role admin from 192.168.0.2	GUREDI 21. Authenticated by login.
8.8.6.default Friday, November 4 2022 16:36:25		○ 00:22:55
Management	IPsec VPN » Connections » (unnamed)	
Network Authentication	General Authentication Firewall IKE Options	
Network Security	Authentication	0
Global	Authentication method X.509 certificate	•
Connections L2TP over IPsec	Local X.509 certificate	
IPsec Status	Remote CA certificate No CA certificate,	out the remote certificate below
QoS Logging Support	Remote certificate ± Download Subject: emailAddress=s	Development Developme
	Issuer: CN=Cer Valid from: No	ificado_CA,OU=PHC,O=PhoenixContact,L=SaoPaulo,ST=SaoPaulo,C=BR
	Valid until: Nov	4 19:33:00 2023 GMT
	Fingerprint MD	5: F6:01:89:27:BC:F3:D3:8E:E2:5A:DC:DA:51:2A:7A:70
	Fingerprint SH	1:94:AD:BE:2E:D5:F4:95:39:45:D4:19:8D:8B:00:ED:49:F5:A3:F9:91
	VPN Identifier	*
Copyright © 2001-2022 PHOENIX CONT	ACT Cyber Security GmbH and others Legal Notice Trademarks & Patents	mGuard Documentation

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.





🔲 🕑 mGuard (mguard)	× +						– o x
\leftarrow $ ightarrow$ \mathbb{C} $$ $$ \mathbb{A} Na	ão seguro https://192.168.0.1/inde					A to t	E Convidado 🕘 …
8.8.6.default	WARNIN Logged in	G: THE ROOT PASSW as admin with role ad	ORD IS NOT CONF min from 192.168.0.2	IGURED! 21. Authenticated by login.			D \$\$
Monday, November 7 2022 15:20:44							₫ 00:28:09
Management I	IPsec VPN » Connections » Shre	wSoft_VPN					
Network	General Authentication	Firewall	IKE Options				
Network Security	ISAKMP SA (Key Exchange))					0
Global	Seq. 🕂	Encryption		Hash		Diffie-Hellman	
Connections L2TP over IPsec	1 🕂 🖬	AES-256	•	SHA-256	•	3072 bits (group 15)	-
IPsec Status OpenVPN Client	IPsec SA (Data Exchange)						
QoS	Seq. (+)	Encryption	I.		Hash		
Support	1 🕂 🗐	AES-256	-		SHA-256	-	
	Perfect Forward Secrecy	(PFS) (Activation	3072 bits (group 1	5)			-
	recommended. The remote s	ite must have the same entry.)					
	Lifetimes and Limits						
	IS	AKMP SA lifetime	8:00:00				seconds (hh:mm:ss)
Copyright © 2001-2022 PHOENIX CONTA	ACT Cyber Security GmbH and others Le	gal Notice Trademarks	& Patents				mGuard Documentation

	WARNING: THE ROOT PASS Logged in as admin with role a	VORD IS NOT CONFIGURED! Imin from 192.168.0.221. Authenticated by login.	日
Monday, November 7 2022 15:22:11			ල් 00:26:42
Management	IPsec VPN » Connections » ShrewSoft_VPN		
Network Authentication	General Authentication Firewall	IKE Options	
Network Security	IPsec SA lifetime	1:00:00	seconds (hh:mm:ss)
IPsec VPN Global	IPsec SA traffic limit	0	bytes
Connections L2TP over IPsec IPsec Status	Re-key margin for lifetimes (applies to ISAKMP SAs and IPsec SAs)	0:09:00	seconds (hh:mm:ss)
OpenVPN Client QoS	Re-key margin for the traffic limit (applies to IPsec SAs only)	0	bytes
Logging Support	Re-key fuzz (applies to all re-key margins)	100	percent
	Keying tries (0 means unlimited tries)	0	
	Dead Peer Detection		
	Delay between requests for a sign of life	0:00:30	seconds (hh:mm:ss)
	Timeout for absent sign of life after which peer is assumed dead	0:02:00	seconds (hh:mm:ss)
			< Back
Copyright © 2001-2022 PHOENIX	CONTACT Cyber Security GmbH and others Legal Notice Trademarks	& Patents	mGuard Documentatio

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

\leftarrow \rightarrow C \textcircled{a} A	Não seguro https://192.168.0.1/index.cgi	A" to	£≦ Convidado ② ···
	WARNING: THE ROOT PASSWORD IS NOT CONFIGURED! Logged in as admin with role admin from 192.168.0.221. Authenticated by login.		
8.8.6.default Monday, November 7 2022 15:36:38			₫ 00:12:15
Management	IPsec VPN » Connections » ShrewSoft_VPN		
Network			

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) VPN Access Manager	-	×
File Edit View Help		
Connect Add Modify Delete		

- 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.

PN Site C	onfiguration			×
General	Client Name R	esolution	Authenticatic *	• •
Remot	e Host			
Host N	lame or IP Addres	s	Port	
mgua	dserver.ddns.net		500	
Auto C	onfiguration	disabled	~	
Local H Adapte	lost er Mode			
Use a	virtual adapter ar	nd assigne	ed address \sim	
мти		🗌 Obtai	n Automatically	
141	4 Address	192.1	68.4.1	
	Netmask	255.2	55 . 255 . 255	
	[Save	Cance	sl –

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

VPN Site Configur	ation	×			
General Client	Name Resolution	Authenticatic • •			
Firewall Option	\$				
NAT Traversa	l er	nable 🗸			
NAT Traversa	l Port	4500			
Keep-alive pa	cket rate	6C Secs			
IKE Fragmentation		nable 🗸			
Maximum pac	ket size	540 Bytes			
Other Options					
🗹 Enable De	ad Peer Detection				
Enable ISAKMP Failure Notifications					
Enable Clie	ent Login Banner				
	Save	e Cancel			





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

Enable DNS Obtain Automatically	DING HINTO
Server Address #1	Cenable WINS Obtain Automatically Server Address #1 Server Address #2
Obtain Automatically DNS Suffix	

- e) Na aba Authentication, configure da seguinte forma:
 - Authentication Method: selecione Mutual RSA.
 - Nas abas Local Identity and Remote Identity, configure conforme figuras abaixos. •
 - 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).

VPN Site Configuration X	VPN Site Configuration	VPN Site Configuration
Client Name Resolution Authentication Phase	Client Name Resolution Authentication Phase	Client Name Resolution Authentication Phase • • • Authentication Method Mutual RSA
Local Identity Remote Identity Credentials Identification Type ASN.1 Distinguished Name ASN.1 DN String	Local Identity Remote Identity Credentials Identification Type ASN.1 Distinguished Name ASN.1 DN String	Local Identity Remote Identity Credentials Server Certificate Autority File Certificade_CA crt Chert Certificate File Chert Certificate File
☑ Use the subject in the client certificate	Use the subject in the received certificate but don't compare it with a specific vaue	Client Private Key File ShrewSoft_Client pem Pre Shared Key
Save Cancel	Save Cancel	Save Cancel

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

Name Resolution Authe	entication Phase I Phase I
Froposal Farameters	
Exchange Type	main 🗸 🗸
DH Exchange	group 15 🛛 🗸
Cipher Algorithm	aes 🗸 🗸
Cipher Key Length	256 V Bits
Hash Algorithm	sha2-256 \sim
Key Life Time limit	28800 Secs
Key Life Data limit	0 Kbytes
Enable Check Point	Compatible Vendor ID
	companyor ronadi ib





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.

(B) VPN Access Manager File Edit View Help	-		×	S VPN Connect - mguar — Connect Network	×
Connect Add Modify Delete		•		attached to key daemon peer configured iskamp proposal configured client configured client configured remote id configured remote id configured client key configured client key configured turnel enabled Disconnect Cancel	~

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.

IPsec 5	Status			
∱ _{Wai}	iting			
ISAKMP	Local	192.168.3.3:500 / C=BR, ST=SP, L=SaoPaulo, O=PhoenixContact, OU=PHC, CN=mGuard_Server, E=suporte@phoenixcontact.com.br	aes-256;sha2-256;modp-	
SA	Remote	%any:500 / C=BR, ST=SP, L=SaoPaulo, O=PhoenixContact, OU=PHC, CN=ShrewSoft_Client, E=suporte@phoenixcontact.com.br	(1024 1536 2048 3072 4096 6144 8192)	
IPsec SA		ShrewSoft_VPN: 192.168.0.0/24192.168.4.1/32	aes-256;(md5 sha1 sha2- (256 384 512))	/
<mark>≻</mark> Pen	nding			
≥ _{Pen}	ading ablished	(
≥ Pen	ablished	(contrine) 192.168.3.3:4500 / C=BR, ST=SP, L=SaoPaulo, O=PhoenixContact, OU=PHC, CN=mGuard_Server, E=suport@phoenixcontact.com.br	main-r3 replace in 53m 24s (active)	
≻ Pen	ablished Local Remote	192.168.3.3:4500 / C=BR, ST=SP, L=SaoPaulo, O=PhoenixContact, OU=PHC, CN=mGuard_Server, E=suporte@phoenixcontact.com.br 152.247.68 117:41264 / C=BR, ST=SP, L=SaoPaulo, O=PhoenixContact, OU=PHC, CN=ShrewSoft_Client, E=suporte@phoenixcontact.com.br	main-r3 replace in 53m 24s (active) — acs-256;sha2-256;modp- (1024 1536 2048 3072 4096 6144 8192)	

