# Publicando o *Remote Desktop* com Microsoft ISA Server 2004.

Autor: Ian Bergmann

#### Introdução:

O Microsoft Windows 2003 Server, assim como o Windows XP, dispõe do recurso de acesso remoto, denominado *Remote Desktop*. Este recurso permite a conexão com computadores de qualquer lugar, utilizando a internet. Como o Microsoft ISA Server 2004 bloqueia por padrão todas as portas, é necessário publicar este serviço para podermos acessar este recurso.

### Pré-requisitos:

- Windows 2000 Server SP4 ou 2003 Server SP1;
- Microsoft ISA Server 2004 SP2 e
- Conexão internet com IP válido.

#### Publicando o Remote Desktop:

- 1. Abra o ISA Server 2004;
- 2. Clique na árvore do console;



Ilustração 1 – Expandir a árvore do console.



3. Selecione Firewall Policy;



Ilustração 2 - Expandir o Firewall Policy.

4. Na aba Tasks, clique em Create New Server Publishing Rule;

rquivo Ação Exibir Ajuda • →   🔁 🔣 😭 🔮   ⋺ 🤆	) 🎯				
Microsoft Internet Security and Accele SISA Monitoring Firewall Policy	Microso Inter Acce Standard	ft <sup>e</sup> net Security & leration Server	2004		Firewall Polic
Virtual Privace Networks (VPN)     E	Firewal	Policy			Toolbox Tasks Help
	0 🔺	Name	Action	Protocols 🔼	
	9 1	W32.Sasser	🚫 Deny	W32.Sasser	Firewall Policy
	9 2	W32.NetSky	🚫 Deny	🔍 W32.NetSky	Tasks
	🥐 3	W32.MyDoom	🚫 Deny	🔍 W32.MyDoom	🐑 Create New Access Rule
	🥐 4	W32.Blaster	🚫 Deny	🔍 W32.Blaster	🐑 Publish a Web Server
	9 5	W32.Bagle	🚫 Deny	🔍 W32.Bagle	Publish a Secure Web
	🖃 💦 6	Bloquear Proxies	. 🚫 Deny		Publish a Mail Server
	🖃 [ 7	Sem filtro	Allow	👯 HTTP sem Filtro	Publishing Rule
	8	RDP IN	Allow	🖳 RDP (Terminal Service	System Policy
		RDP IN Servidor	Allow	RDP (Terminal Service	Tasks
	🖃 💽 10	Skype	Allow	HTTPS	Edit System Policy
	🖃 💽 11	Acesso ao FTP	Allow	🔍 FTP 🔽	Export System Policy
	<	1111		>	Import System Policy

Ilustração 3 – Create a New Server Publishing Rule.



5. Escolha um nome sugestivo para a nova regra, e depois clique em *Avançar*;

New Server Publishing Ru	le Wizard 🛛 🔀		
Microsoft Internet Security & Acceleration Server 2004	Welcome to the New Server Publishing Rule Wizard This wizard helps you create a new server publishing rule. Server publishing rules map incoming client requests to the appropriate internal server.		
	<u>S</u> erver publishing rule name: RDP IN To continue, click Next.		
	< Voltar Avançar > Cancelar		

Ilustração 4 – Nomeando a nova regra.

6. Coloque o endereço IP do servidor que será publicado, em seguida clique *Avançar*;

New Server Publishing Rule Wizard	×
Select Server Specify the network IP address of the server you are publishing.	
<u>S</u> erver IP address:	
10 . 1 . 1 . 250 Browse	
	Cancelar

Ilustração 5 – Atribuindo endereço IP do servidor a ser publicado.



7. No campo Selected Protocol escolha o protocolo RDP (Terminal Services) Server, em seguida, caso deseje alterar a porta (por padrão é a 3389), clique no botão Ports;

New Server Publishing Rule Wizard	
Select Protocol Select the protocol used by the published server.	
Selected protocol:	
RDP (Terminal Services) Server	Properties
	Ports
	Ne <u>w</u>
	Cancelar

Ilustração 6 - Selecionando protocolo.

8. A alteração da porta é duplamente desejável: Segurança, já que um possível invasor terá que descobrir além do IP a porta utilizada; e a possibilidade de publicar vários servidores. Após alterar a porta clique *OK* e em seguida *Avançar*;

Ports	?
The port override options let you override the default ports us to the published server.	ed to connect
Help about overriding default ports	
Firewall Ports	
O Publish using the default port defined in the protocol defined	nition
• Publish on this port instead of the default port:	55001
Published Server Ports	
• <u>Send requests to the default port on the published serve</u>	r
○ Send requests to this port on the published server:	÷
Source Ports	
⊙ Allow traffic from any allowed source port	
$\bigcirc$ Limit access to traffic from this range of source ports:	
Erom:	\$
This range must belong to clients specified in the allowe sources for this rule.	ed traffic

Ilustração 7 – Alterando a porta de publicação.



9. O passo seguinte é escolher em qual rede vamos publicar o servidor. Como desejamos que seja para a internet, no campo *Listen for requests* from these networks selecionamos *External*, depois *Avançar*;

Addresses Select the network IP addresses on	the ISA Server that will listen for rea	iests
intended for the published server.		
isten for requests from these networks:		
Name	Selected IPs	~
🗹 📥 External 🖌	<all addresses="" ip=""></all>	
📃 📥 Internal	<all addresses="" ip=""></all>	
📃 👍 Local Host	<all addresses="" ip=""></all>	
📃 👍 Quarantined VPN Clients	<all addresses="" ip=""></all>	
📃 📥 VPN Clients	<all addresses="" ip=""></all>	V
< ]		>
		Address
	< ⊻oltar Avançar:	Canc

Ilustração 8 – Selecionando a rede para publicação do Remote Desktop.

10. Pressione Concluir para finalizar;

ew server Publishing Ru	le wizaro
Microsoft Internet Security & Acceleration Server 2004	Completing the New Server Publishing Rule Wizard You have successfully completed the New Server Publishing Rule Wizard. The new Server Publishing Rule will have the following configuration:
	Name: RDP IN Published Server: 10.1.250 Published Service: RDP (Terminal Services) Server Listen on: External
	×
	< >
	To close the wizard, click Finish.
	<ul> <li>Voltar</li> <li>Concluir</li> <li>Cancelar</li> </ul>

Ilustração 9 – Concluindo.



11. Clique em Apply para aplicar as configurações;

🖾 Microsoft Internet Security and	Accelera	tion Server 2004					X
Arquivo Açã <u>o</u> Exibir Aj <u>u</u> da							
← → 🗈 🖬 😤 🔄 📭 🕈	× ⊛ €	) 🗣 🎓 🅃 🍃					
Microsoft Internet Security and Accele     SISA     Monitoring     Griewall Policy     Virtual Private Networks (VPN)     Griguration	Microsof Intern Accel Standard	ft net Security & leration Server: Edition Apply Disc	2004 ard 1	o save changes and upda	te the	Firewall Polic	;y
	Firewall	Policy				Toolbox Tasks Help	
	0 🔺	Name	Action	Protocols	^		^
	🥐 1	W32.Sasser	🚫 Deny	🖳 W32.Sasser		Firewall Policy	
	🥐 2	W32.NetSky	🚫 Deny	🔍 W32.NetSky	=	Tasks	
	9 3	W32.MyDoom	🚫 Deny	👰 W32.MyDoom		Create New Access Rule	
	<b>?</b> 4	W32.Blaster	🚫 Deny	🔍 W32.Blaster	-	🐑 Publish a Web Server	=
	<b>?</b> 5	W32.Bagle	O Deny	🔍 W32.Bagle	ſ	Publish a Secure Web	
	<b>= 💦</b> 6	Bloquear Proxies	🚫 Deny		ľ	Server	
	🖃 🎊 7	Sem filtro	Allow	👯 HTTP sem Filtro		Publishing Rule	
	8	RDP IN	🕢 Allow	🖳 RDP (Terminal Service	e	X Delete Selected Rules	
	<u> </u>	RDP IN Servidor	<b>Allow</b>	RDP (Terminal Service	e	Move Selected Rules Up	
	🖃 💓 10	Skype	Allow	<b>I</b> II HTTPS	~	Move Selected Rules Down	
	<	Ш		× >		Disable Selected Rules	~
	,						

Ilustração 10 – Aplicando as configurações criadas.

12. OK para finalizar.



Até este ponto fizemos o trabalho de publicação do serviço de acesso remoto, porém o Isa Server 2004, por padrão, não libera a publicação de computadores da rede. Se o servidor que você publicou é o próprio ISA, não encontrará nenhuma dificuldade de conexão após os passos acima. Entretanto, se você publicou um outro servidor, é necessário que libere o acesso ao mesmo, conforme descrito na seqüência a seguir.



13. Vá novamente em *Firewall Policy* e clique com o botão direito do mouse e selecione *Edit System Policy*;



Ilustração 12 – Abrindo o editor do System Policy.

14. Localize e clique no *Terminal Server*, localizado na coluna *Configuration Groups*. Em *General* confirme se está habilitado (*Enable*), logo após clique na tab *From*;



Ilustração 13 - Habilitando o Terminal Service.



15. Na tab *From*, localize a regra *Remote Management Computers*, marque-a e selecione o botão *Edit*;

Configuration Groups	General From	
<ul> <li>Network Services</li> <li>DHCP</li> <li>DNS</li> <li>NTP</li> <li>Authentication Services</li> <li>Active Directory</li> <li>RADIUS</li> <li>RSA SecurID</li> <li>CRL Download</li> <li>Remote Management</li> <li>Microsoft Management</li> <li>Microsoft Management</li> <li>Terminal Server</li> <li>ICMP (Ping)</li> <li>Firewall Client</li> <li>Firewall Client Install</li> </ul>	This rule applies to traffic from these sources:  Remote Management Computers  Exceptions:	Add Edit Remove Add
<ul> <li>Diagnostic Services         ICMP         Windows Networking         Microsoft Error Repc         HTTP Connectivity v     </li> </ul>		Edit Remove

Ilustração 14 – Editando a regra Remote Management Computers.

16. Abrirá então a janela de configuração do *Remote Management Computers*. Você verá que não existe nenhum computador ou rede configurada;

eral	
Name:	Remote Management Computers
iomputers, addr et:	ress ranges and subnets included in this computer
Name	IP Addresses

Ilustração 15 - Regra padrão, sem computador ou rede configurada.



17. Selecione *Add*, e observe que é possível adicionar um computador, um escopo de endereços IP ou uma subrede. No exemplo abaixo foi adicionado uma subrede;

neral		
Nam	e: Remote Management Compute	rs
Computers,	address ranges and subnets included in thi	s computer
2.2	1	1
Name	Docal 10.1.1.0/24	
Name	IP Addresses	
Name	IP Addresses ocal 10.1.1.0/24 Add Edit Delet	3
Name	IP Addresses       bcal     10.1.1.0/24       Add     Edit       Computer     Address Range	3

Ilustração 16 – Incluindo um computador, escopo de endereços ou uma subrede.

18. Clique em OK para voltar à janela do System Policy Editor;

eral	
Name:	Remote Management Computers
Iomputers, address jet:	ranges and subnets included in this computer
Name	IP Addresses
Rede Local	10.1.1.0/24
Adg	. Edit Delete
optional):	remotely

Ilustração 17 – Confirmando a alteração.



19. Novamente em OK para fechar o System Policy Editor;

Configuration Groups General From	
<ul> <li>Network Services DHCP DNS NTP</li> <li>Authentication Services Active Directory RADIUS RSA SecurID CRL Download</li> <li>Remote Management Microsoft Management Microsoft Management Firewall Client Firewall Client Install</li> <li>Diagnostic Services ICMP Windows Networkinç Microsoft Error Repc HTTP Connectivity v</li> <li>Logging</li> </ul>	Add Edit Remove

Ilustração 18 – Fechando o System Policy Editor.

20. Clique em Apply para aplicar as configurações.

<u>A</u> rquivo Açã <u>o</u> E <u>x</u> ibir Aj <u>u</u> da							
← →   🖻 💽 😫 🔮 🚰	× ⊛ €	) 🔹 🌢 🅃					
Microsoft Internet Security and Accele     SISA     Monitoring     Firewall Policy     Virtual Private Networks (VPN)     S Configuration	Microso Inter Acce Standan	ft <sup>e</sup> net Security & leration Server dEdition Apply Disc	2004 :ard 1	o save changes and upd	late the c	Firewall Poli	сy
	Firewal	Policy				Toolbox Tasks Help	
	0 🔺	Name	Action	Protocols	^		Ţ
	9 1	W32.Sasser	🚫 Deny	🖳 W32.Sasser		Firewall Policy	
	<b>?</b> 2	W32.NetSky	🚫 Deny	🔍 W32.NetSky	Ξ	Tasks	
	<b>?</b> 3	W32.MyDoom	🚫 Deny	👯 W32.MyDoom		Ereate New Access Rule	
	<b>?</b> 4	W32.Blaster	🚫 Deny	🖳 W32.Blaster		🛅 Publish a Web Server	
		W32.Bagle	O Deny	🖳 W32.Bagle	Π	😑 Publish a Secure Web	
	🖃 [ 6	Bloquear Proxies	. 🚫 Deny		ð	Server Publish a Mail Server	
	🖃 [ 7	Sem filtro	🕜 Allow	👯 HTTP sem Filtro		Publishing Rule	
	8 (5)	RDP IN	🕢 Allow	🖳 RDP (Terminal Serv	ice	X Delete Selected Rules	
	<u>[]</u> 9	RDP IN Servidor	🖉 Allow	RDP (Terminal Serv	ice	Move Selected Rules Up	
	🖃 🎅 10	Skype	Allow	<b>I</b> II HTTPS	~	Move Selected Rules Down	
	<	101		· · ·	>	( Disable Selected Rules	1

Ilustração 19 - Aplicando as configurações criadas.



#### 21. OK para finalizar.



Para fazer a conexão ao servidor publicado, deve-se utilizar o aplicativo *Conexão da área de trabalho remota*, disponíveis nos Windows 2003/XP. Se você alterou a porta de publicação do *Remote Desktop*, além do endereço IP para conexão, acrescente dois pontos (:) seguido da porta utilizada, como no exemplo abaixo.

🕄 Conexão	de área de trabalho remota 🛛 🖃 🖾
	Área de trabalho remota Conexão
Computador:	200.254.254.1:65001
	Conectar-se Cancelar Ajuda Opções >>

Ilustração 21 - Conectando ao servidor publicado.

## Conclusão:

Quando executamos os passos descritos acima, disponibilizamos o acesso remoto a servidores e/ou computadores da rede pela internet, de qualquer lugar do planeta. Este recurso permite uma gama de aplicações, como administração da rede, disponibilizar recursos para usuários fora do ambiente da empresa, manutenção e muitas outras possibilidades. Entretanto, devemos lembrar que todo recursos de acesso remoto, seja pelo Remote Desktop, por uma VPN, ou outro software qualquer, aumenta a possibilidade de um ataque obter sucesso. Por isso devemos tomar cuidados extras com a segurança, evitando a divulgação do IP e portas de conexão, exigindo senhas seguras e com tempo de vida reduzido entre outros.

