Bloqueando o Messenger com Filtro de HTTP no Microsoft ISA Server 2004.

Autor: Ian Bergmann

Introdução:

Muitas vezes o uso do Messenger em uma empresa torna-se indesejável, neste momento temos que tomar as medidas necessárias para evitá-lo. Como já sabemos, a simples proibição não basta, é preciso impedir que os usuários possam fazê-lo. Uma maneira eficaz é a utilização do filtro de HTTP no Microsoft® Internet Security and Acceleration (ISA) Server 2004. Este tutoria visa justamente orientar em tal tarefa.

Bloqueando o Messenger:

Para efetuar o bloqueio do Messenger em uma rede utilizando o Microsoft ISA Server 2004, deve-se criar uma nova regra no filtro de http. Consiste na verificação do conteúdo do cabeçalho da mensagem, conforme os passos descritos abaixo:

- 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.

 Na regra de acesso a internet, clique com o botão direito do mouse e escolha "Configure HTTP";

🖾 Microsoft Internet Security and	Acceleration Server 20	104				_	
<u>A</u> rquivo Açã <u>o</u> E <u>x</u> ibir Ajuda							
	' X	2					
Microsoft Internet Security and Accele SISA Monitoring Monitoring Sirewall Policy	Microsoft Internet Security & Acceleration Server Standard Edition	Firewall Policy					
Virtual Private Networks (VPN) Configuration	Firewall Policy				Toolbox Tasks Help		
B-X-Congulation	O 🔺 Name	Action	Protocols	^	Protoco	ls	8
	🖃 📝 10 RDP OUT	⊘ Allow	🖳 RDP (Terminal	Service	Users		8
	🖃 💽 11 Rede Local	Allow	All Outbound 1		Content	t Types	8
				.raffic	<u>S</u> chedul	les	۲
	🖃 💽 12 SMTP	🥝 Allow 🔋	👰 SMTP		Networ	<u>k</u> Objects	0
					New • Edit Delete		
	🖃 💽 13 POP3	🕝 Allow	100 рорз	, ,			
	= 🥐 14 Internet	🕜 Allow		Properties Delete		s Ranges s	
	🖃 💽 15 Sites da Lana	i Allow	HTTP HTTPS HTTPS Serve	Сору	ter Sets ts Selected Name Sets		
				Export Sel			
	😲 Last Default rule	🚫 Deny	💐 All Traffic	import to selected		-	
				Move Dow Move Up Disable	iove Down Iove Up Disable		
				Configure	нттр 📥	-	
Concluído				configure			

Ilustração 3 – Abrindo a opção de configuração do protocolo HTTP.

5. Selecione a Tab "Signatures";



Ilustração 4 – Janela de configuração de Assinaturas.

6. Clique no botão "Add" para adicionar um novo filtro;



Ilustração 5 - Adicionando um novo filtro de Assinatura.

7. Na janela Signatures preencha conforme demonstrado nos exemplos, mais abaixo, e depois confirme em OK;

lamou					
<u>v</u> ame.	Live Messenger				
oescription (optional):	Filtro para bloqueio do Microsoft Live Messenger				
Signature Search	Criteria				
Search in:	Request headers				
HTTP header:	User-agent				
Specify the signal	ure to block:				
≦ignature:	Live Messenger				
	- Byte range	Format			
	Erom: 1	Text			
	To:	C Binary			

Ilustração 6 - Modelo do filtro de Assinaturas para o Messenger.

8. Clique no botão Aplicar para confirmar a alteração;



Ilustração 7 – Aplicando a nova regra.

9. Confirme em Apply na tela principal do ISA.

🖽 Microsoft Internet Security and	Acceleration Server 20	104		2	
<u>A</u> rquivo Açã <u>o</u> E <u>x</u> ibir Aj <u>u</u> da					
← → 🗈 🖬 😫 🗿 🗳 🖀	X 🏵 🔄 🔹 🕥 🖇	2			
Microsoft Internet Security and Accele SISA Monitoring Firewall Policy Virtual Private Networks (VPN)	Microsoft ⁻ Internet Security & Acceleration Server Standard Edition	data uka ang Gamatia	Firewall Policy		
⊕ 🔆 Configuration	Арру С	date the configuration	, сіск арріу.		
	Firewall Policy	Toolbox	Tasks Help		
	O 🔺 Name	Action Protocols	Protoc	ols 🛞	
	I0 RDP OUT	Allow RDP (Terminal Service Allow RU All Outbound Traffic	vice <u>U</u> sers	8	
			Conter	t Types 🛞	
			fic <u>S</u> chedu	ıles 🛞	
			Netwo	k Objects 🛞	
	🖃 💽 12 SMTP	🕜 Allow 🛛 🖳 SMTP	New - Ed	it <u>D</u> elete	
	🖃 💽 13 POP3	a m	> 🗄 🧰 Nel	works	
		Allow 🕎 POP3	👝 🛛 🕀 🚞 Nel	work Sets	
		A	Co	nputers	
	= 14 Internet	Allow HTTP	Adi 🔁 Sui	dress Ranges	
		@	E Con	mets mouter Sets	
	🖃 🥂 15 Sites da Lana		🕀 🚞 UR	L Sets	
		MTTPS Server	💷 🗉 🗀 Dor	nain Name Sets	
	Last Default rule	O Deny 🛄 All Traffic	we	b Listeners	
			>		

Ilustração 8 - Salvando as alterações no ISA.

Observe que para cada versão do Messenger existe uma assinatura diferente, como mostrado demonstrado a seguir:

Messenger 7.5:

Name: MSN Messenger Search in: Request headers HTTP header: User-agent Signature: MSN Messenger Messenger Live:

Name: Live Messenger Search in: Request headers HTTP header: User-agent Signature: Live Messenger

Onde:

- Name: Nome da regra. Pode-se usar o nome do aplicativo e sua versão. Aqui usei o nome MSN Messenger e Live Messenger.
- Description: Opcional. Como o nome já diz, é uma descrição do filtro criado.
- Search In: Indica tipo de mensagem que o filtro deve verificar, neste caso é o Request headers.
- http header: Quando aplicável, especifica qual campo do cabeçalho deve ser analisado. Neste exemplo é o User-agent. User-agent é um dos parâmetros do cabeçalho do protocolo HTTP que identifica o cliente que inicia uma requisição. Normalmente os navegadores (Internet Explorer, Opera, Firefox...), aplicativos de mensagens instantâneas (MSN, AIM, Skype...), ou qualquer outra aplicação utilizada pelo usuário final na internet.
- Signature: É a assinatura da aplicação, que se identifica pelo nome e pela versão do software. No nosso caso MSN Messenger e Live Messenger.

Conclusão:

Neste tutorial demonstrei como bloquear o Messenger utilizando filtros de aplicação do Microsoft ISA Server 2004. Podemos efetuar este tipo de bloqueio em diversos aplicativos diferentes. Alguns cabeçalhos utilizados pelas aplicações mais comuns podem ser encontrados no site da Microsoft TechNet <u>http://www.microsoft.com/technet/isa/2004/plan/commonapplicationsignatures.</u> <u>mspx</u> (em inglês).