O Uso de Firewalls na Segurança de Redes

Thiago Silvino 25/11/2013

Fundação Bradesco Campinas

Palestrante

Thiago Silvino www.silvino.net

Especialista em Segurança de Redes – AT&T www.att.com

Atua na área de redes de computadores desde 2002

Objetivo da Palestra

Temas abordados:

- 1 Conceitos de redes de computadores
- 2 Equipamentos de rede
- 3 Funcionamento de firewalls
- 4 Packet filtering e stateful inspection
- 5 Antispoofing
- 6 NAT e VPNs

Redes de Computadores

Interconexão entre equipamentos
Transmissor, meio de transmissão e receptor
Envio e recebimento de informações
Compartilhamento de recursos (discos, arquivos, conexões)

Modelos de rede TCP/IP e OSI

Equipamento	Unidade	TCP/IP	OSI		
Firewall, proxy,	Dados	5. Aplicação	7. Aplicação		
loadbalancer			6. Apresentação		
			5. Sessão		
	Segmento	4. Transporte	4. Transporte		
Roteadores	Pacote/datagrama	3. Rede	3. Rede		
Switches e bridges	Quadro	2. Enlaçe	2. Enlaçe		
Hub, Cabos e conectores	Bit	1. Física	1. Física		

Equipamentos de rede

Para interconectar os computadores podemos usar vários equipamentos

- 1 Switches e access-points: usados para fazer a conexão física das placas de rede
- 2 Roteadores: utilizados para encaminhar pacotes entre várias redes
- 3 Firewalls: usados para interligar as redes de forma segura

Endereçamento de rede

Exemplo de endereçamento de uma placa de rede sem fio

Property	Value
Connection-specifi	
Description	Intel(R) Centrino(R) Advanced-N 6205
Physical Address	8C-70-5A-1D-02-34
DHCP Enabled	Yes
IPv4 Address	192.168.0.14
IPv4 Subnet Mask	255.255.255.0

Topologia de rede

Firewall

- Usando um firewall podemos criar regras de acesso para as suas redes
- Cada regra define os endereços de origem (quem inicia a comunicação), endereços de destino (qual endereço será acessado), protocolos e ação (ACCEPT, DROP, REJECT)
- O firewall olha a tabela de regras de cima para baixo e aplica a primeira que se aplicar a conexão

Tipos de firewall

1 – Filtro de pacotes

Nesse tipo de firewall devemos definir regras em todas as interfaces de rede do firewall. Devemos criar regras específicas para garantir o retorno dos pacotes.

2 – Stateful inspection

Um firewall com a tecnologia stateful inspection usa uma tabela de conexões para garantir o retorno dos pacotes. A empresa Check Point patenteou essa tecnologia e a incluiu no seu produto FireWall-1 em 1994.

Ferramentas: Firewall CheckPoint

Principais programas do SmartConsole:

- SmartDashboard: tabela de regras de segurança, NAT, Application & URL Filtering, Data Loss Prevention, IPSec VPN e QOS.
- SmartView Tracker: Visualização de Logs
- SmartMonitor: Monitoração de status dos firewalls
- SmartUpdate: Upgrade de software e manutenção de licenças e contratos

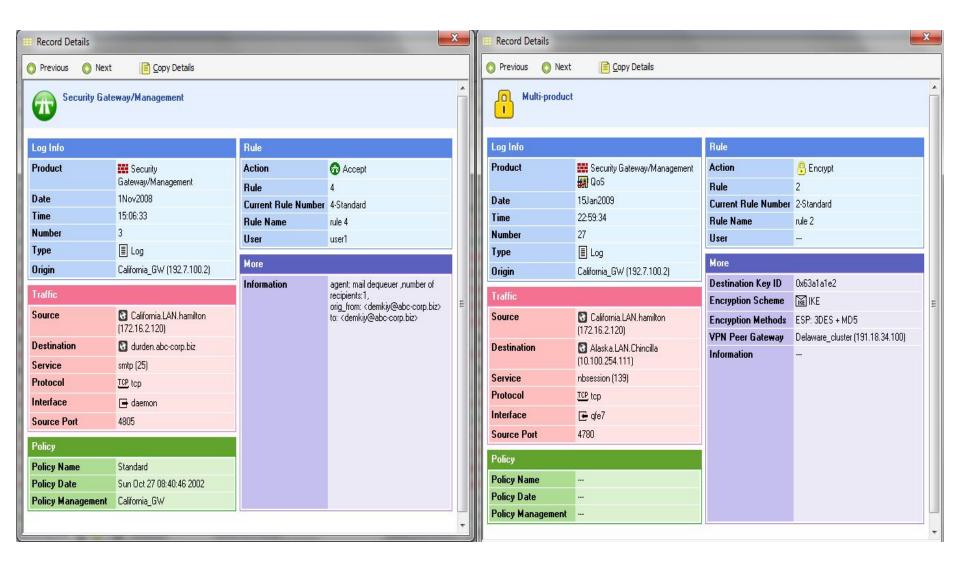
Exemplo: SmartDashboard

No.	Hits	Name	Source	Destination	VPN	Service	Action		Install On	Time	Comment	
-	Limit Acc	ess to Gateways F	Rule (Rule 1)									
1	0	Stealth	★ Corporate-internal-net	⊞ GW-group	★ Any Traffic	★ Any	odrop	Alert	Policy Targets	★ Any	Stealth rule - prevent the VPN _fire host from being scanned or attack	
+	VPN Acce	ess Rules (Rules	2-5)		Na Para	\	iii	W .	\tag{4}	*	**	
Ξ	Rules for	Specific Sites (F	Rules 6-8)			4						
6	111 21K	Outbound HTTP	₩ Remote-2-internal	★ Any	Any Traffic	TCP http	Client Auth	Log	Remote-2-gw	★ Any	Audit all outbound user HTTP connections remote-2-internal using UserAuthority	
7	1 47K	Critical subnet	← Corporate-internal-net	→ Corporate-finance-net → Corporate-hr-net → Corporate-rnd-net	★ Any Traffic	★ Any	accept	Log	Corporate-gw	★ Any	Log traffic to critical subnets - only enforce this rule on the Corporate-g	
8	ш зк	Tech support	Tech-Support	Remote-1-web-server	Any Traffic	TCP http	accept accept	Alert	Remote-1-gw	★ Any	Allow technical support access to v server - only enforce this rule on Remote-1-gw	
+	Identity B	lased Access (Ru	ules 9-12)									
Е	Common I	Rules - All Sites	(Rules 13-19)		v)	VI.	W.	W.	W.		w	
13	4M	Terminal server	Corporate-internal-terminal-server	★ Any	Any Traffic	★ Any	Session Auth	Log	Corporate-gw	★ Any	Audit all traffic from terminal server using UserAuthority	
14	□ 2K	DNS server	★ Any	Corporate-dns-ext	★ Any Traffic	UDP domain-udp	accept accept	- None	Policy Targets	★ Any	Allow domain name queries to exter DNS server	
15	672K	SOAP	★ Any	Corporate-WA-proxy-server	★ Any Traffic	HTTP http->SOAP-requests	accept accept	Log	Policy Targets	★ Any	Allow only selected SOAP methods block all others	
16	0	Mail and Web servers	★ Any	Corporate-dmz-net	★ Any Traffic	TCP http TCP https TCP smtp	accept	Log	★ Policy Targets	★ Any	Allow incoming connections to the mand web servers	
17	663K	SMTP	Corporate-mail-server	Internal-net-group	Any Traffic	TCP smtp	accept accept	Log	Policy Targets	★ Any	Allow outgoing SMTP connections, t don't allow the mail server to initiate connections to the internal networks case it is compromised	
18	Ⅲ 66K	DMZ and Internet	Internal-net-group	★ Any	Any Traffic	₩ Any	accept accept	Log	Policy Targets	★ Any	User access to DMZ servers and Inf	
19	3M	Clean up rule	★ Any	★ Any	Any Traffic	★ Any	o drop	Log	Policy Targets	★ Any	Clean up rule - block all other connections	

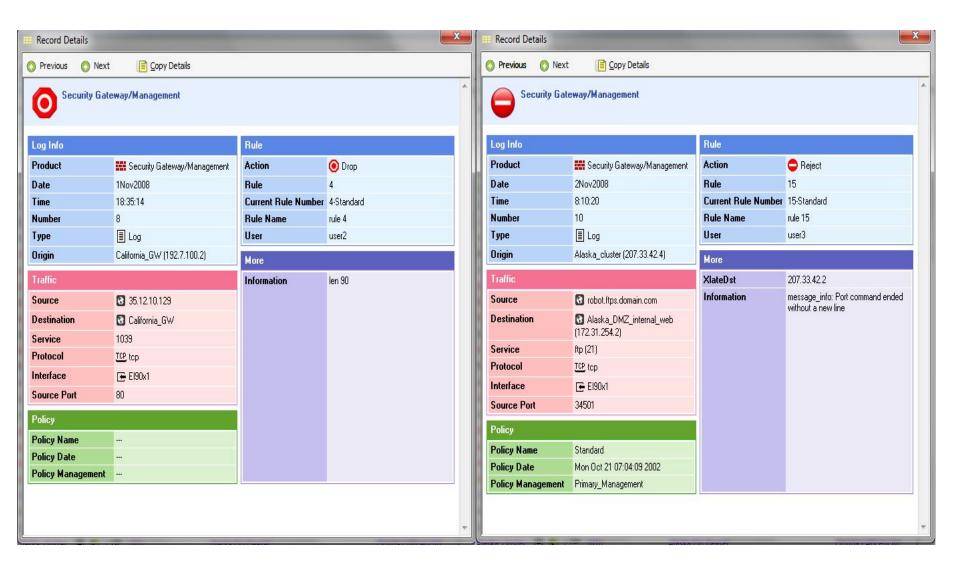
Exemplo: SmartView Tracker

Network & Endpoint Q		abc 🚣 🗏	1 X	A	+											- 5
Predefined	No.	▼ Date	▼ Time	YY	▼ Origin	YY	Y	▼ Service	▼ Source	▼ Source User Name	▼ Destination	▼ Rule	▼ Curr. Rule	▼ Rule Na	▼ Source Port	₹ User
All Records	1	1Nov2008	1:11:29		Alaska_mem	4										user1
Network Securit	2	1Nov2008	15:00:41	₩ 🕒	California_GW		, TCP	smtp	California.LAN.ha		durden.abc-corp.biz	4	4-Standard	rule 4	4805	user1
🗓 📵 Firewall Blad	3	1Nov2008	15:06:33		California_GW		TCP	smtp	California.LAN.ha		durden.abc-corp.biz	4	4-Standard	rule 4	4805	user1
⊕ ▼ IPS Blade	4	1Nov2008	15:41:29	 •	California_GW		TCP	smtp	California.LAN.ku		California_GW	4	4-Standard	rule 4	2972	user2
Application :	5	1Nov2008	16:43:13	₩ 🕒	California_GW		, <u>UDP</u>	sip	voip		California_GW	3	3-Standard	rule 3	10008	user2
⊕ ∰ HTTPS Inspe	6	1Nov2008	17:43:28		California_GW		1									user2
⊕ Anti-Bot & A	7	1Nov2008	18:35:11		California_GW		TCP	smtp	California.LAN.jac		pc1.abc-hq.com1	10	10-Standard	rule 10	2693	user2
H Identity Awa	8	1Nov2008	18:35:14		California_GW		TCP	1039	35.12.10.129		California_GW	4	4-Standard	rule 4	80	user2
⊕ 🚳 Anti-Spam 8	9	1Nov2008	18:39:42	E	Alaska_RND		, <u>TCP</u>	http	10.111.254.11		www.ietf.org	12	12-Standard	rule 12	1208	user3
Mobile Acce	10	2Nov2008	8:10:20		Alaska_cluster		TCP	ftp	robot.ftps.domain		Alaska_DMZ_inter	15	15-Standard	rule 15	34501	user3
Data Loss Pro	11	2Nov2008	8:11:22	***	Alaska_cluster		TCP	ftp	robot.ftps.domain		Alaska_DMZ_inter	15	15-Standard	rule 15	34555	user3
⊕ ⊕ IPSEC VPN B	12	2Nov2008	8:11:30	****			TCP	ftp	robot.ftps.domain		Alaska_DMZ_inter	15	15-Standard	rule 15	34497	user3
	13	2Nov2008	8:12:29	-	Alaska_cluster		TCP	ftp	robot.ftps.domain		Alaska_DMZ_inter	15	15-Standard	rule 15	34533	user3
Advanced N	14	2Nov2008	8:14:36	 E	Alaska_cluster		TCP	ftp	robot.ftps.domain		Alaska_DMZ_inter	15	15-Standard	rule 15	35421	user3
⊕ ⊕ Traditional A	15	2Nov2008	8:14:38		Alaska_mem	4										
🗓 👨 Voice over IF	16	3Nov2008	11:14:26		Alaska_cluster		TCP	ftp	robot.ftps.domain		Alaska_DMZ_inter	15	15-Standard	rule 15	34533	user4
⊕ More	17	15Mar2009	1:00:1		Primary_Man	4										
Firewall-1 G	18	15Mar2009	2:14:36	E	Alaska_cluster		TCP	http	resolved.hosts.com		Alaska_DMZ_inter	0	0-Standard	Implied rule	35421	user4
	12	15Mar2009	2:19:21	:::: E	Alaska_Finan		TCP	microsoft-ds	Alaska.IT.Bentli		10.112.254.9	11	11-Standard	rule 11	32818	user4
Monitoring E	20	15Mar2009	10:9:29		The second secon		, <u>TCP</u>	8080	10.111.254.31	Jennifer McHanry (j	192.168.9.111	12	12-Standard	rule 12	32818	user5
🖃 🎉 Endpoint Securit	21	15Mar2009	10:9:30		Alaska_RND		TCP	8080	10.111.254.31	Jennifer McHanry (j	192.168.9.111	0	0-Standard	Implied rule	32822	user6
	22	15Mar2009	10:9:31	 E	Alaska_RND		TCP	8080	10.111.254.31	Jennifer McHanry (j	192.168.9.111	0	0-Standard	Implied rule	32822	user4
Compliance	23	16Mar2009	16:35:14	****	Company of the Compan		TCP	http	scriptskids.inc		Alaska_DMZ_inter	14	14-Standard	rule 14	1208	user4
	24	16Mar2009	16:35:19	E	Alaska_cluster		TCP	http-81	scriptskids.inc		Alaska_DMZ_inter	14	14-Standard	rule 14	1208	user4
- 👸 Blocked Prog	25	1Jan2009	22:54:13	E	Alaska_cluster	■ 0-			California.LAN.jac		Alaska_cluster					MR. TES
	26	1Jan2009	22:54:13	E	 3 ************************************	L.			California.LAN.jac			0	0-Standard	Implied rule		MR. TES
<u> </u>	27	151an2000	22-50-24	· 🕞	California GW		I TCP	nheerion	California I ANI ha		Alacka I ANI Chinci	2	2-Standard	rule 2	1780	

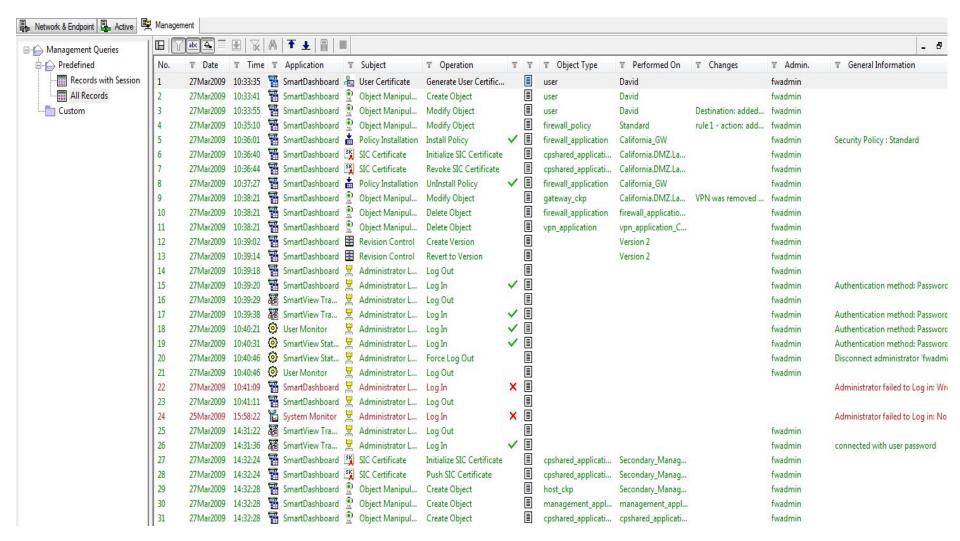
Exemplo: SmartView Tracker accept



Exemplo: SmartView Tracker drop



Exemplo: SmartView Tracker admin



Antispoofing

Usando a técnica de address spoofing um computador de uma rede externa tenta se passar por uma máquina de uma rede interna modificando o IP de origem de um pacote.

Configuração de Antispoofing

