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, loadbalancer	Dados	5. Aplicação	7. Aplicação
			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

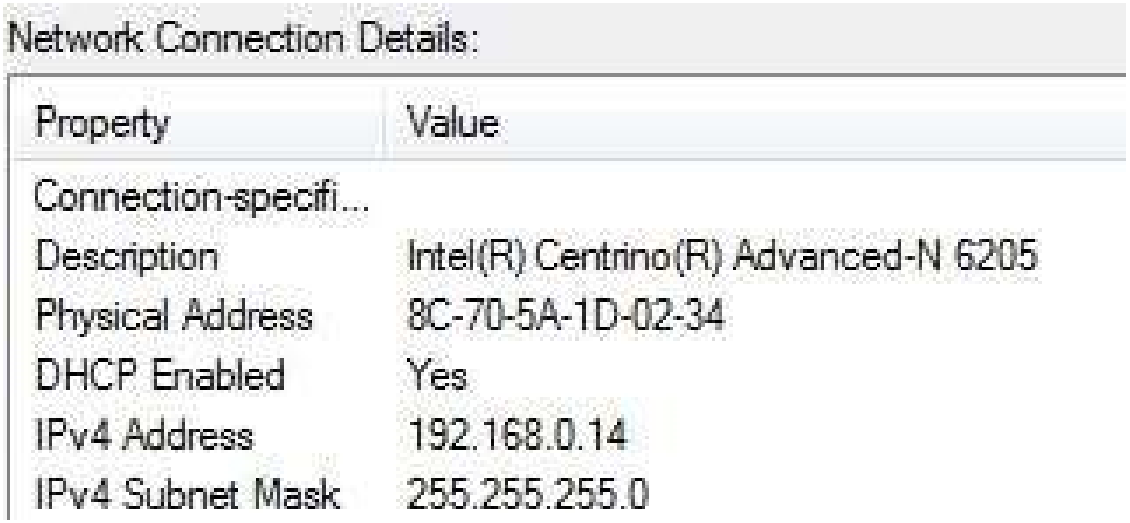
1 – Switches e access-points: usados para fazer a conexão física das placas de rede

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



Network Connection Details:

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

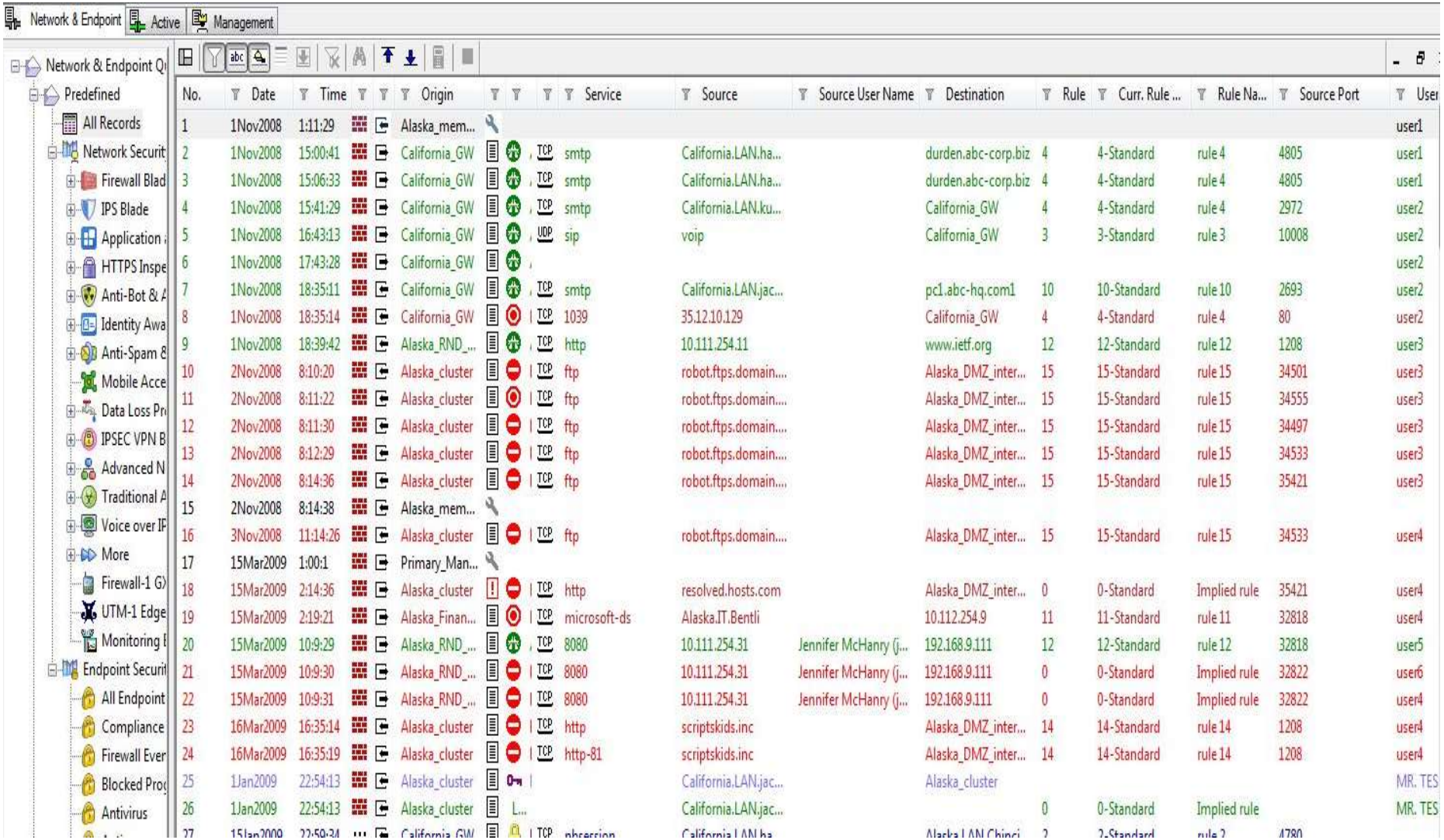
Principais programas do SmartConsole:

- 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

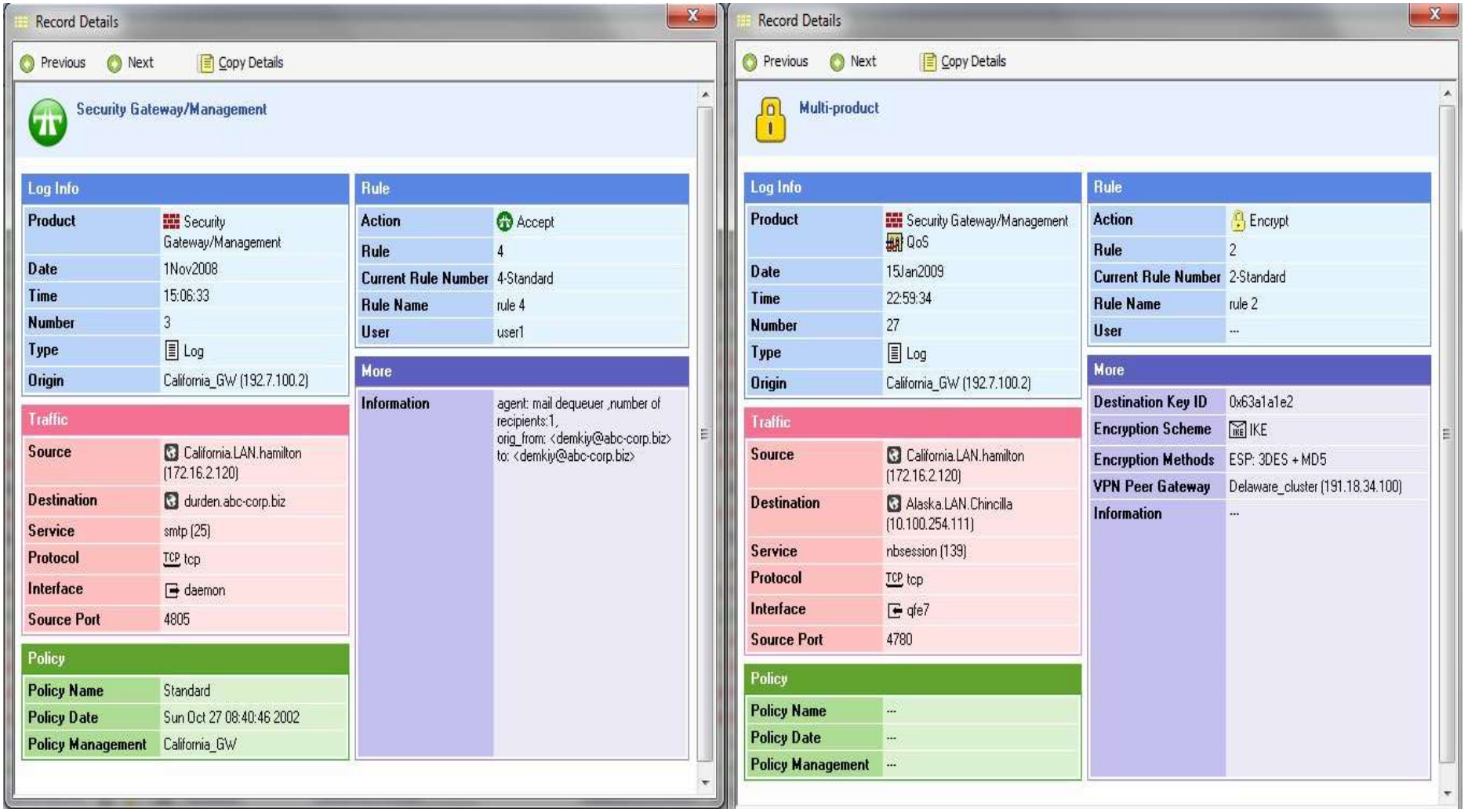
Exemplo: SmartDashboard

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time	Comment
	Limit Access to Gateways Rule (Rule 1)										
1	0	Stealth	Corporate-internal-net	GW-group	Any Traffic	Any	drop	Alert	Policy Targets	Any	Stealth rule - prevent the VPN _firew host from being scanned or attacke
	VPN Access Rules (Rules 2-5)										
	Rules for Specific Sites (Rules 6-8)										
6	21K	Outbound HTTP	Remote-2-internal	Any	Any Traffic	http	Client Auth	Log	Remote-2-gw	Any	Audit all outbound user HTTP conne from remote-2-internal using UserAuthority
7	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	3K	Tech support	Tech-Support	Remote-1-web-server	Any Traffic	http	accept	Alert	Remote-1-gw	Any	Allow technical support access to v server - only enforce this rule on Remote-1-gw
	Identity Based Access (Rules 9-12)										
	Common Rules - All Sites (Rules 13-19)										
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	domain-udp	accept	None	Policy Targets	Any	Allow domain name queries to exter DNS server
15	672K	SOAP	Any	Corporate-WA-proxy-server	Any Traffic	http->SOAP-requests	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	http https smtp	accept	Log	Policy Targets	Any	Allow incoming connections to the m and web servers
17	663K	SMTP	Corporate-mail-server	Internal-net-group	Any Traffic	smtp	accept	Log	Policy Targets	Any	Allow outgoing SMTP connections, b don't allow the mail server to initiate connections to the internal networks case it is compromised
18	66K	DMZ and Internet	Internal-net-group	Any	Any Traffic	Any	accept	Log	Policy Targets	Any	User access to DMZ servers and Int
19	3M	Clean up rule	Any	Any	Any Traffic	Any	drop	Log	Policy Targets	Any	Clean up rule - block all other connections

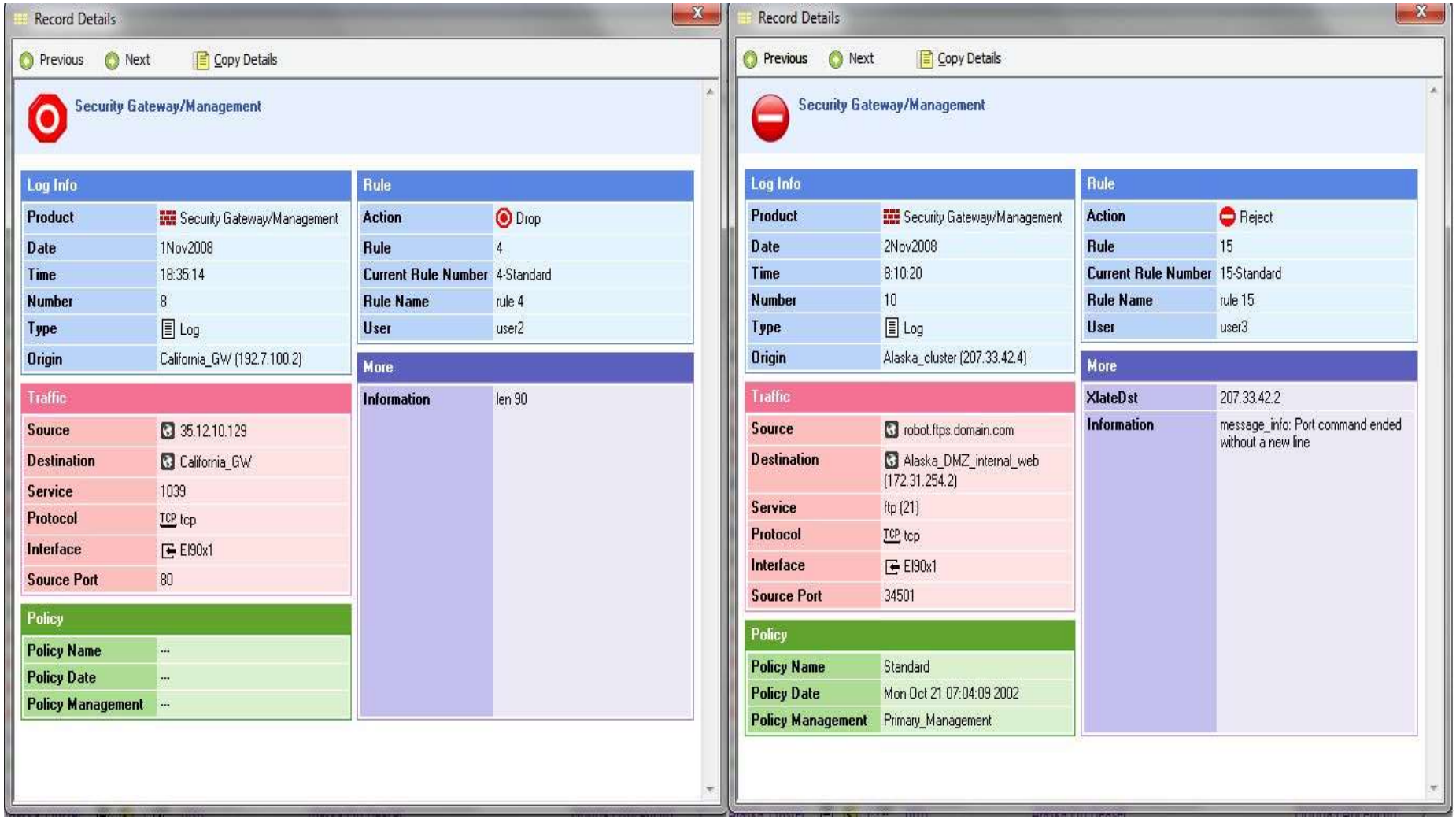
Exemplo: SmartView Tracker



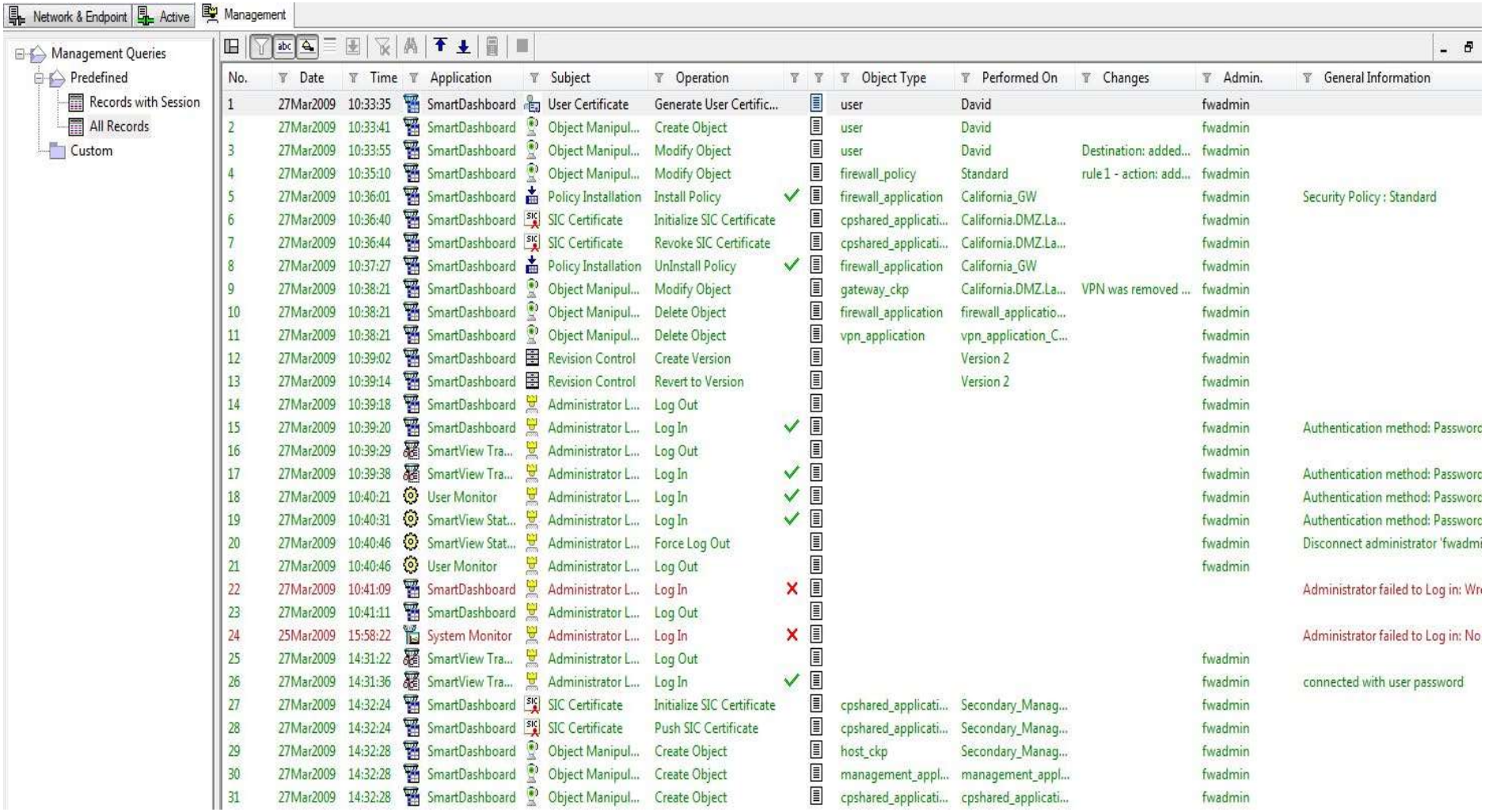
Exemplo: SmartView Tracker accept



Exemplo: SmartView Tracker drop



Exemplo: SmartView Tracker admin



No.	Date	Time	Application	Subject	Operation		Object Type	Performed On	Changes	Admin.	General Information
1	27Mar2009	10:33:35	SmartDashboard	User Certificate	Generate User Certific...		user	David		fwadmin	
2	27Mar2009	10:33:41	SmartDashboard	Object Manipul...	Create Object		user	David		fwadmin	
3	27Mar2009	10:33:55	SmartDashboard	Object Manipul...	Modify Object		user	David	Destination: added...	fwadmin	
4	27Mar2009	10:35:10	SmartDashboard	Object Manipul...	Modify Object		firewall_policy	Standard	rule 1 - action: add...	fwadmin	
5	27Mar2009	10:36:01	SmartDashboard	Policy Installation	Install Policy	✓	firewall_application	California_GW		fwadmin	Security Policy : Standard
6	27Mar2009	10:36:40	SmartDashboard	SIC Certificate	Initialize SIC Certificate		cpshared_applicati...	California.DMZ.La...		fwadmin	
7	27Mar2009	10:36:44	SmartDashboard	SIC Certificate	Revoke SIC Certificate		cpshared_applicati...	California.DMZ.La...		fwadmin	
8	27Mar2009	10:37:27	SmartDashboard	Policy Installation	UnInstall Policy	✓	firewall_application	California_GW		fwadmin	
9	27Mar2009	10:38:21	SmartDashboard	Object Manipul...	Modify Object		gateway_ckp	California.DMZ.La...	VPN was removed ...	fwadmin	
10	27Mar2009	10:38:21	SmartDashboard	Object Manipul...	Delete Object		firewall_application	firewall_applicatio...		fwadmin	
11	27Mar2009	10:38:21	SmartDashboard	Object Manipul...	Delete Object		vpn_application	vpn_application_C...		fwadmin	
12	27Mar2009	10:39:02	SmartDashboard	Revision Control	Create Version			Version 2		fwadmin	
13	27Mar2009	10:39:14	SmartDashboard	Revision Control	Revert to Version			Version 2		fwadmin	
14	27Mar2009	10:39:18	SmartDashboard	Administrator L...	Log Out					fwadmin	
15	27Mar2009	10:39:20	SmartDashboard	Administrator L...	Log In	✓				fwadmin	Authentication method: Password
16	27Mar2009	10:39:29	SmartView Tra...	Administrator L...	Log Out					fwadmin	
17	27Mar2009	10:39:38	SmartView Tra...	Administrator L...	Log In	✓				fwadmin	Authentication method: Password
18	27Mar2009	10:40:21	User Monitor	Administrator L...	Log In	✓				fwadmin	Authentication method: Password
19	27Mar2009	10:40:31	SmartView Stat...	Administrator L...	Log In	✓				fwadmin	Authentication method: Password
20	27Mar2009	10:40:46	SmartView Stat...	Administrator L...	Force Log Out					fwadmin	Disconnect administrator 'fwadmi
21	27Mar2009	10:40:46	User Monitor	Administrator L...	Log Out					fwadmin	
22	27Mar2009	10:41:09	SmartDashboard	Administrator L...	Log In	✗					Administrator failed to Log in: Wr
23	27Mar2009	10:41:11	SmartDashboard	Administrator L...	Log Out						
24	25Mar2009	15:58:22	System Monitor	Administrator L...	Log In	✗					Administrator failed to Log in: No
25	27Mar2009	14:31:22	SmartView Tra...	Administrator L...	Log Out					fwadmin	
26	27Mar2009	14:31:36	SmartView Tra...	Administrator L...	Log In	✓				fwadmin	connected with user password
27	27Mar2009	14:32:24	SmartDashboard	SIC Certificate	Initialize SIC Certificate		cpshared_applicati...	Secondary_Manag...		fwadmin	
28	27Mar2009	14:32:24	SmartDashboard	SIC Certificate	Push SIC Certificate		cpshared_applicati...	Secondary_Manag...		fwadmin	
29	27Mar2009	14:32:28	SmartDashboard	Object Manipul...	Create Object		host_ckp	Secondary_Manag...		fwadmin	
30	27Mar2009	14:32:28	SmartDashboard	Object Manipul...	Create Object		management_appl...	management_appl...		fwadmin	
31	27Mar2009	14:32:28	SmartDashboard	Object Manipul...	Create Object		cpshared_applicati...	cpshared_applicati...		fwadmin	

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