

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-specific...	
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 ,frew host from being scanned or attacked
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 conner 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-IWA-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, t 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



Network & Endpoint Management																
Network & Endpoint Q																
Predefined																
All Records																
Network Security																
Firewall Blade																
IPS Blade																
Application																
HTTPS Inspe																
Anti-Bot & A																
Identity Awa																
Anti-Spam &																
Mobile Acce																
Data Loss Pn																
IPSEC VPN B																
Advanced N																
Traditional A																
Voice over IP																
More																
Firewall-1 G																
UTM-1 Edge																
Monitoring t																
Endpoint Security																
All Endpoint																
Compliance																
Firewall Ever																
Blocked Prog																
Antivirus																
No.	Date	Time	Origin	Service	Source	Source User Name	Destination	Rule	Curr. Rule ...	Rule Na...	Source Port	User				
1	1Nov2008	1:11:29	Alaska_mem...									user1				
2	1Nov2008	15:00:41	California_GW	TCP smtp	California.LAN.ha...		durden.abc-corp.biz	4	4-Standard	rule 4	4805	user1				
3	1Nov2008	15:06:33	California_GW	TCP smtp	California.LAN.ha...		durden.abc-corp.biz	4	4-Standard	rule 4	4805	user1				
4	1Nov2008	15:41:29	California_GW	TCP smtp	California.LAN.ku...		California_GW	4	4-Standard	rule 4	2972	user2				
5	1Nov2008	16:43:13	California_GW	UDP sip	voip		California_GW	3	3-Standard	rule 3	10008	user2				
6	1Nov2008	17:43:28	California_GW									user2				
7	1Nov2008	18:35:11	California_GW	TCP smtp	California.LAN.jac...		pc1.abc-hq.com1	10	10-Standard	rule 10	2693	user2				
8	1Nov2008	18:35:14	California_GW	TCP 1039	35.12.10.129		California_GW	4	4-Standard	rule 4	80	user2				
9	1Nov2008	18:39:42	Alaska_RND...	TCP http	10.111.254.11		www.ietf.org	12	12-Standard	rule 12	1208	user3				
10	2Nov2008	8:10:20	Alaska_cluster	TCP ftp	robot.ftp.domain...		Alaska_DMZ_inter...	15	15-Standard	rule 15	34501	user3				
11	2Nov2008	8:11:22	Alaska_cluster	TCP ftp	robot.ftp.domain...		Alaska_DMZ_inter...	15	15-Standard	rule 15	34555	user3				
12	2Nov2008	8:11:30	Alaska_cluster	TCP ftp	robot.ftp.domain...		Alaska_DMZ_inter...	15	15-Standard	rule 15	34497	user3				
13	2Nov2008	8:12:29	Alaska_cluster	TCP ftp	robot.ftp.domain...		Alaska_DMZ_inter...	15	15-Standard	rule 15	34533	user3				
14	2Nov2008	8:14:36	Alaska_cluster	TCP ftp	robot.ftp.domain...		Alaska_DMZ_inter...	15	15-Standard	rule 15	35421	user3				
15	2Nov2008	8:14:38	Alaska_mem...													
16	3Nov2008	11:14:26	Alaska_cluster	TCP ftp	robot.ftp.domain...		Alaska_DMZ_inter...	15	15-Standard	rule 15	34533	user4				
17	15Mar2009	1:00:1	Primary_Man...													
18	15Mar2009	2:14:36	Alaska_cluster	TCP http	resolved.hosts.com		Alaska_DMZ_inter...	0	0-Standard	Implied rule	35421	user4				
19	15Mar2009	2:19:21	Alaska_Finan...	TCP microsoft-ds	Alaska.IT.Bentli		10.112.254.9	11	11-Standard	rule 11	32818	user4				
20	15Mar2009	10:9:29	Alaska_RND...	TCP 8080	10.111.254.31	Jennifer McHanry (j...	192.168.9.111	12	12-Standard	rule 12	32818	user5				
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	Alaska_RND...	TCP 8080	10.111.254.31	Jennifer McHanry (j...	192.168.9.111	0	0-Standard	Implied rule	32822	user4				
23	16Mar2009	16:35:14	Alaska_cluster	TCP http	scriptskids.inc		Alaska_DMZ_inter...	14	14-Standard	rule 14	1208	user4				
24	16Mar2009	16:35:19	Alaska_cluster	TCP http-81	scriptskids.inc		Alaska_DMZ_inter...	14	14-Standard	rule 14	1208	user4				
25	1Jan2009	22:54:13	Alaska_cluster		California.LAN.jac...		Alaska_cluster					MR. TES				
26	1Jan2009	22:54:13	Alaska_cluster	L...	California.LAN.jac...			0	0-Standard	Implied rule		MR. TES				
27	15Jan2009	22:50:24	California_GW	TCP nhraccon	California.LAN.ha...		Alaska.LAN.Chinci	2	2-Standard	rule 2	4780					





Exemplo: SmartView Tracker accept

Record Details


Previous Next Copy Details

 Security Gateway/Management

Log Info	
Product	 Security Gateway/Management
Date	1Nov2008
Time	15:06:33
Number	3
Type	 Log
Origin	California_GW (192.7.100.2)

Traffic	
Source	 California.LAN.hamilton (172.16.2.120)
Destination	 durden.abc-corp.biz
Service	smtp (25)
Protocol	 tcp
Interface	 daemon
Source Port	4805

Policy	
Policy Name	Standard
Policy Date	Sun Oct 27 08:40:46 2002
Policy Management	California_GW

Rule	
Action	 Accept
Rule	4
Current Rule Number	4-Standard
Rule Name	rule 4
User	user1


More




Information





agent: mail dequeuer ,number of recipients:1, orig_from: <demkiy@abc-corp.biz> to: <demkiy@abc-corp.biz>

Record Details


Previous Next Copy Details

 Multi-product

Log Info	
Product	 Security Gateway/Management
	 QoS
Date	15Jan2009
Time	22:59:34
Number	27
Type	 Log
Origin	California_GW (192.7.100.2)

Traffic	
Source	 California.LAN.hamilton (172.16.2.120)
Destination	 Alaska.LAN.Chincilla (10.100.254.111)
Service	nbssession (139)
Protocol	 tcp
Interface	 qfe7
Source Port	4780

Policy	
Policy Name	---
Policy Date	---
Policy Management	---


Rule	
Action	 Encrypt
Rule	2
Current Rule Number	2-Standard
Rule Name	rule 2
User	---

More

Destination Key ID

0x63a1a1e2

Encryption Scheme

 IKE

Encryption Methods

ESP: 3DES + MD5

VPN Peer Gateway


Delaware_cluster (191.18.34.100)




Information





Exemplo: SmartView Tracker drop

Record Details

Previous Next Copy Details

 Security Gateway/Management

Log Info		Rule	
Product	 Security Gateway/Management	Action	 Drop
Date	1Nov2008	Rule	4
Time	18:35:14	Current Rule Number	4-Standard
Number	8	Rule Name	rule 4
Type	 Log	User	user2
Origin	California_GW (192.7.100.2)		

Traffic	
Source	 35.12.10.129
Destination	 California_GW
Service	1039
Protocol	 tcp
Interface	 E190x1
Source Port	80

Policy	
Policy Name	---
Policy Date	---
Policy Management	---

More	
Information	len 90

Record Details

Previous Next Copy Details

 Security Gateway/Management

Log Info		Rule	
Product	 Security Gateway/Management	Action	 Reject
Date	2Nov2008	Rule	15
Time	8:10:20	Current Rule Number	15-Standard
Number	10	Rule Name	rule 15
Type	 Log	User	user3
Origin	Alaska_cluster (207.33.42.4)		

Traffic	
Source	 robot.ftp.domain.com
Destination	 Alaska_DMZ_internal_web (172.31.254.2)
Service	ftp (21)
Protocol	 tcp
Interface	 E190x1
Source Port	34501

Policy	
Policy Name	Standard
Policy Date	Mon Oct 21 07:04:09 2002
Policy Management	Primary_Management

More	
XlateDst	207.33.42.2
Information	message_info: Port command ended without a new line

Exemplo: SmartView Tracker admin

Network & Endpoint Active Management											
Management Queries											
<ul style="list-style-type: none"> Predefined <ul style="list-style-type: none"> Records with Session All Records Custom 											
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_applicati...		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: Wn
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

Check Point Gateway - Corporate-gw

General Properties

- Topology
- ISP Redundancy
- Proxy
- NAT
- HTTPS Inspection
- HTTP/HTTPS Proxy
- Anti-Bot and Anti-Virus
- Platform Portal
- Identity Awareness
- UserCheck
- IPS
- IPSec VPN
- Data Loss Prevention
- Monitoring Software bl
- Logs
- Capacity Optimization
- Hit Count
- Other

Topology

Get...

Name	Network Type	IP Address	Network Mask	Topology
eth0	External	143.100.75.1	255.255.255.0	External
eth1	Internal	172.16.2.1	255.255.255.0	This Network
eth2	Internal	172.16.1.1	255.255.255.0	Marketing
eth3	Internal	10.1.0.1	255.255.255.0	This Network
eth4	Internal	10.2.0.1	255.255.255.0	This Network
eth5	Internal	10.3.0.1	255.255.255.0	This Network

Note: IPv6 address configuration is available in each interface's edit dialog box.

Add... Edit... Remove

VPN Domain

☒ All IP Addresses behind Gateway are based on Topology information

☐ Manually defined

Set domain for Remote Access Community ...

OK Cancel

☒ External (leads out to the Internet)

☐ Internal (leads to the local network)

IP Addresses behind this interface:

☐ Not Defined

☐ Network defined by the interface IP and Net Mask

☐ Specific: View...

☐ Interface leads to DMZ

Anti-Spoofing

☒ Perform Anti-Spoofing based on interface topology

Anti-Spoofing action is set to

☐ Don't check packets from: View...

Spoof Tracking: ☐ None ☒ Log ☐ Alert

☐ External (leads out to the Internet)

☒ Internal (leads to the local network)

IP Addresses behind this interface:

☐ Not Defined

☐ Network defined by the interface IP and Net Mask

☒ Specific: View...

☐ Interface leads to DMZ

Anti-Spoofing

☒ Perform Anti-Spoofing based on interface topology

Anti-Spoofing action is set to

☐ Don't check packets from: View...

Spoof Tracking: ☐ None ☒ Log ☐ Alert