



Lancement d'une attaque par saturation du serveur de messagerie (Mail Flooding)

Les points sensibles : Les SERVEURS



• Serveurs : Web

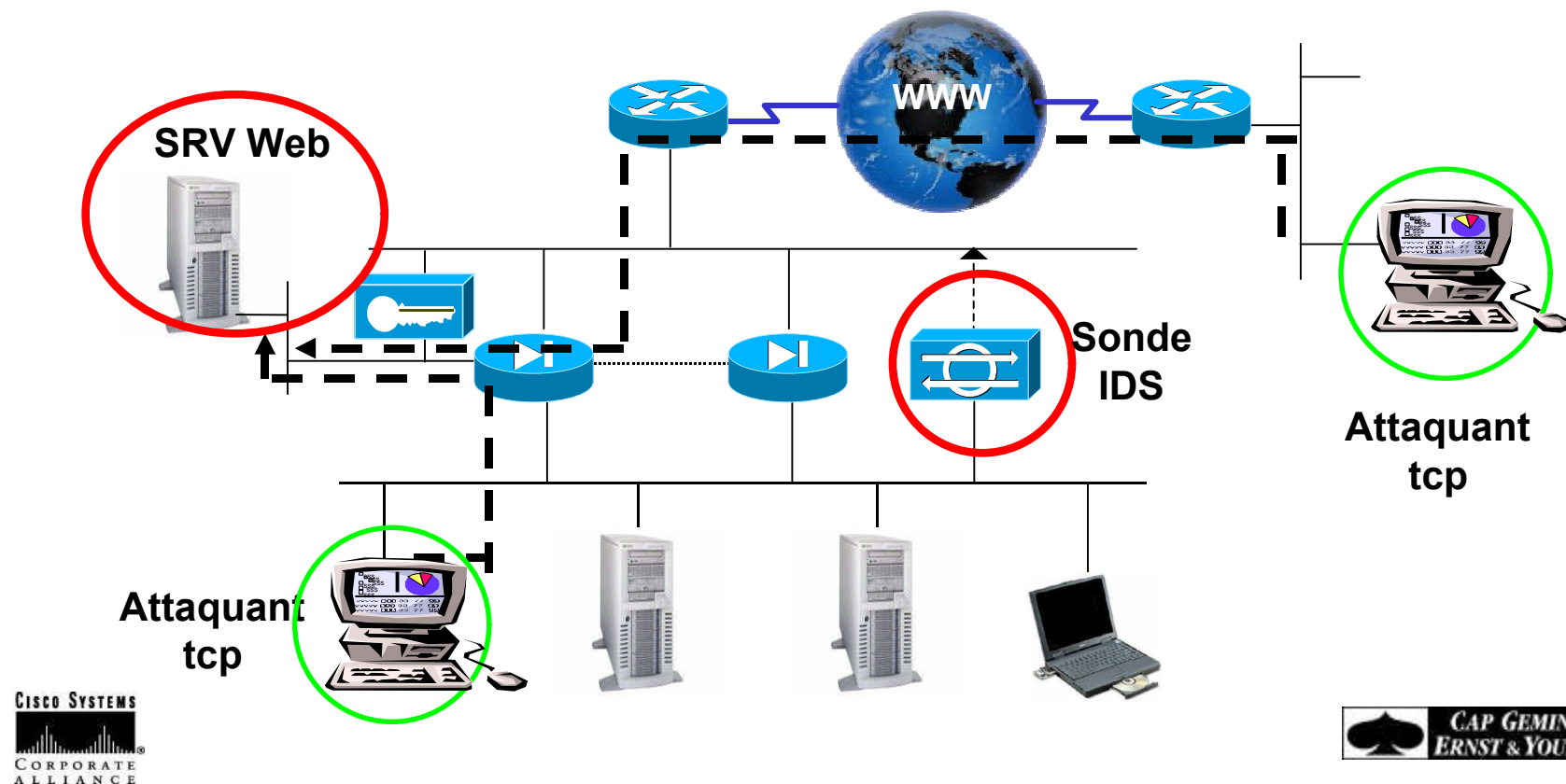


**Attaque de serveur Web par
Deni de service de type
Syn Flood**

Attaque du serveur web de type SYN FLOOD TCP (DOS)



La quantité importante de demandes d'ouvertures de sessions ou demies sessions tcp simultanées, va provoquer une saturation du serveur.
Le pix firewall ou routeur ios fw et la sonde IDS vont stopper cette attaque.



TCP syn flood suite ...PIX

Embryonic limit



- Paramétrage du pix firewall
- Activation des Fonctions IDS sur le Pix

Commandes :

- Nat (inside) id nat, S add, mask, nbre session max, EM limit
- Static(inside,oustside) proto add globale port add local port session max EM limit

Cisco Pix Firewall



Exemples : Firewall Cisco Pix, os 6.2 outils d'administration PDM 2 (Pix Device Manager)



Cisco Pix Firewall 515 E



Cisco Pix 535

Le PIX Firewall outre ses performances et qualités de firewall statefull , de vpn ipsec, offre des fonctions de détections d'intrusion intéressantes.



Lancement de diverses ATTAQUES via SecurScan NX de la société Vigilante

Analyse par la Sonde de Détection d’Intrusion Cisco

Et les fonctions ids du Pix Firewall

Blocage de l'attaque par la sonde afin qu'elle bloque la source ip, au niveau du routeur ou du Cisco Pix firewall



Cisco Systems IDS Device Manager - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History

Address <https://172.28.249.1/cgi-bin/idm>

CISCO SYSTEMS

IDS Device Manager

Logout Apply Changes Help NSDB About

Device Configuration Monitoring Administration

Sensing Engine Communications Logging Blocking Restore Defaults

BACK TO: Configuration Sensing Engine Signature Configuration Signature Groups

TOC

- Signature Configuration
 - Signature Groups**
 - Custom Signatures
 - TCP Connection Signatures
 - UDP Connection Signatures
 - String Signatures
 - ACL Policy Violations
 - STATE HTTP Service Ports
 - Level Of Traffic Logging
 - Filters
 - Filtered Signatures
 - Excluded BO Ports
 - Spam Control
 - Reassembly Options
 - IP Fragment Reassembly
 - TCP Session Reassembly
 - Internal Networks
 - Data Sources
 - Sensing Properties

Editing

Engine	ATOMIC ICMP
Signature	ICMP Echo Reply
Id	2000
Severity	Information
Action	<input type="checkbox"/> Block <input type="checkbox"/> IP Log <input type="checkbox"/> TCP Reset
Comments	ICMP Echo Reply
SubSig	
AlarmInterval [20-3600]	
AlarmThrottle	Summarize
ChokeThreshold	100
FlipAddr	<input type="radio"/> True <input type="radio"/> False <input checked="" type="radio"/> None
IcmpCode	
IcmpId	
IcmpMaxCode	
IcmpMaxSeq	
IcmpMinCode	
IcmpMinSeq	

Info

Select
Signat
view t
individ
signat
select
signat
to view
signat
assoc
that gr
clear
indical
signat
signat
are cu
enable
circle
that al
are er
partial
indical
least c
signat
profile

CISCO SYSTEMS
CORPORATE ALLIANCE

CAP GEMINI
ERNST & YOUNG

Les points sensibles : la bande passante



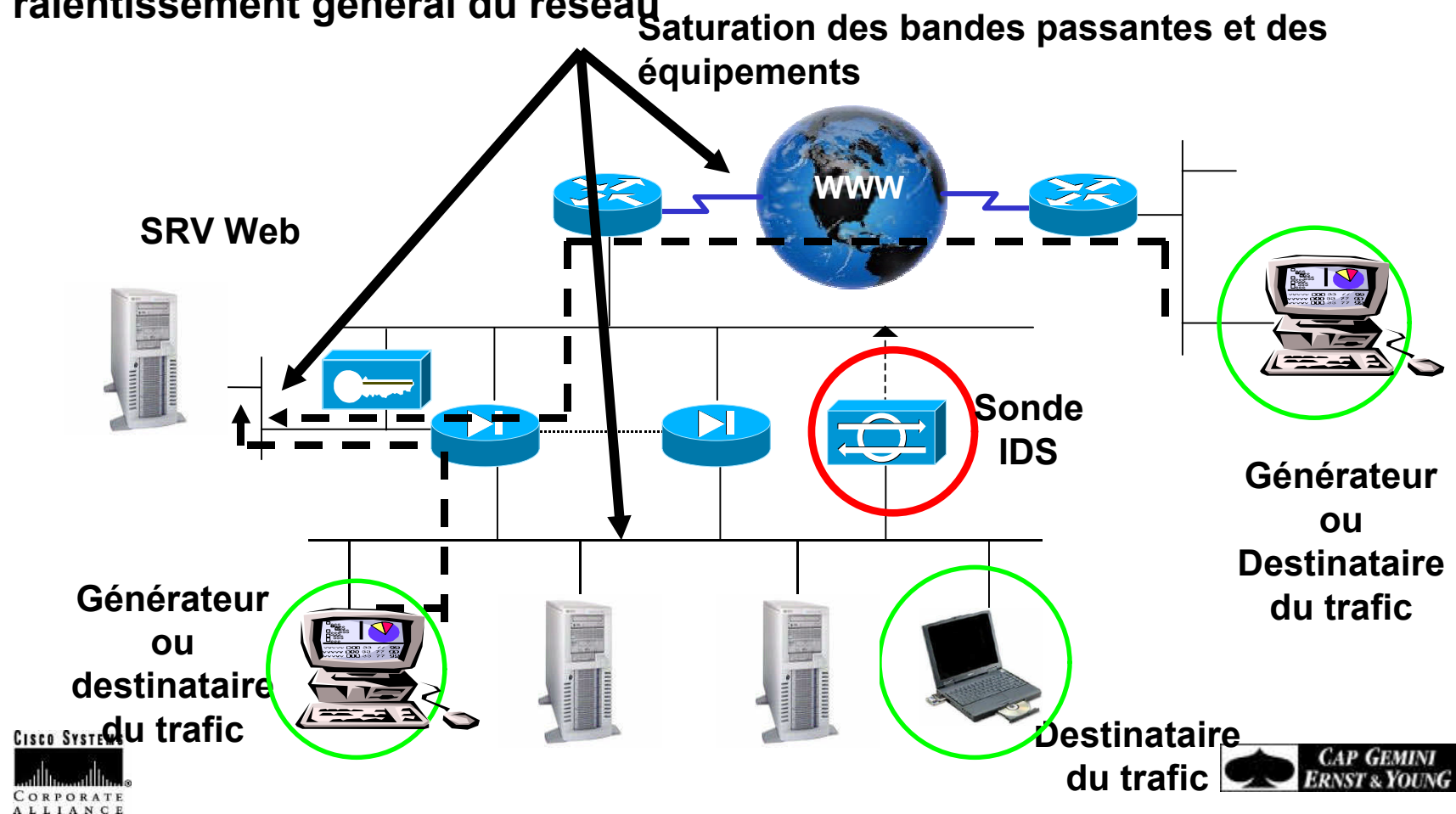
Dans un but de déni de service, la saturation de la bande passante ou des équipements peut être trop facilement exploitée.

De nombreux petits outils existent, permettant de saturer le réseau, en masquant même l'adresse ip source de l'attaquant.

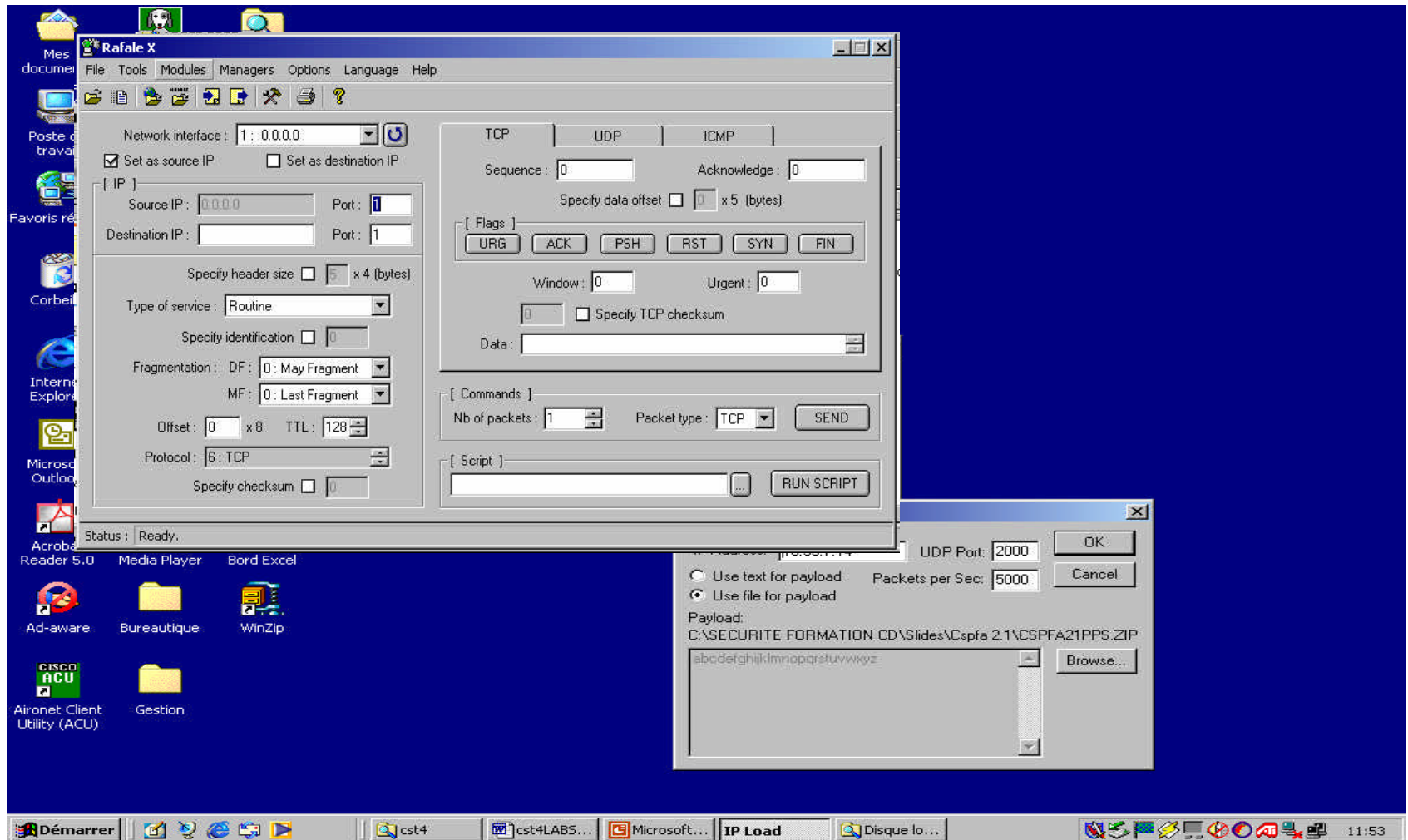
Saturation des bandes passantes



Le Déni de service sur la bande passante, peut être provoquée sur le lan,
Mais également dans le cadre de l'intranet, et peut provoquer un
ralentissement général du réseau



Saturation des bandes passantes...outils



La sonde Cisco IDS



Cisco IDS 4210

Performance 45 Mbps

Attack Protection

Sweeps/floods

DoS¹ mitigation

Worms/viruses

CGI²/WWW attacks

ETC

Buffer overflow protection

RPC attack detection

IP fragmentation attacks

ICMP³ attacks



Cisco IDS 4235

ou 4250

200 Mbps

500 Mbps

SMTP⁴/Sendmail/IMAP⁵/POP⁶ attacks

FTP⁷, SSH⁸, Telnet, and rlogin attacks

DNS⁹ attacks

TCP hijacks



Demo : Affichage des remontées d'alarmes de la sonde Cisco ids 4235

- IDS DEVICE MANAGER**
- IEV Ids Event Viewer**

Les points sensibles : les équipements réseau



Switchs : VTP DOMAIN, telnet



**capture du nom de domain vtp afin
d'injecter ou supprimer les vlans et
capture des passwords telnet et
enable du switch**

Demo vtp, telnet



Capture de trames - VTP Domain (vlan trunk protocol) - Telnet

Visualisation des noms et mot de passe sur une connexion telnet



Sniffer - cartePCMCIA, Ethernet (Line speed at 10 Mbps)

File Monitor Capture Display Tools Database Window Help

Default

Sniftnetswitch: Decode, 1775 Ethernet Frames

No.	Status	Source Address	Dest Address	Summary
1	M	[10.33.7.71]	[10.33.4.53]	TCP: D=23 S=4140 SYN SEQ=2468036424 LEN=0 WIN=16384
2		[10.33.4.53]	[10.33.7.71]	TCP: D=4140 S=23 SYN ACK=2468036425 SEQ=2261254657 LEN=0 WIN=4096
3		[10.33.7.71]	[10.33.4.53]	TCP: D=23 S=4140 ACK=2261254658 WIN=17520
4		[10.33.4.53]	[10.33.7.71]	Telnet: R PORT=4140 IAC Will Echo
5		[10.33.7.71]	[10.33.4.53]	Telnet: C PORT=4140 IAC Do Echo
6		[10.33.4.53]	[10.33.7.71]	Telnet: R PORT=4140 <0D0A0D0A>Cisco Systems, Inc. Console<0D0A0D0A>
7		[10.33.7.71]	[10.33.4.53]	Telnet: C PORT=4140 IAC Do Suppress go-ahead
8		[10.33.4.53]	[10.33.7.71]	TCP: D=4140 S=23 ACK=2468036434 WIN=4096
9		[10.33.7.71]	[10.33.4.53]	Telnet: C PORT=4140 a
10		[10.33.4.53]	[10.33.7.71]	Telnet: R PORT=4140 IAC Will Echo
11		[10.33.7.71]	[10.33.4.53]	Telnet: C PORT=4140 IAC Won't Echo
12		[10.33.4.53]	[10.33.7.71]	TCP: D=4140 S=23 ACK=2468036438 WIN=4096
13		[10.33.7.71]	[10.33.4.53]	Telnet: C PORT=4140 z
14		[10.33.4.53]	[10.33.7.71]	TCP: D=4140 S=23 ACK=2468036439 WIN=4096
15		[10.33.7.71]	[10.33.4.53]	Telnet: C PORT=4140 p
16		[10.33.4.53]	[10.33.7.71]	TCP: D=4140 S=23 ACK=2468036440 WIN=4096
17		[10.33.7.71]	[10.33.4.53]	Telnet: C PORT=4140 a
18		[10.33.4.53]	[10.33.7.71]	TCP: D=4140 S=23 ACK=2468036441 WIN=4096
19		[10.33.7.71]	[10.33.4.53]	Telnet: C PORT=4140 s
20		[10.33.4.53]	[10.33.7.71]	TCP: D=4140 S=23 ACK=2468036442 WIN=4096
21		[10.33.7.71]	[10.33.4.53]	Telnet: C PORT=4140 s
22		[10.33.4.53]	[10.33.7.71]	TCP: D=4140 S=23 ACK=2468036443 WIN=4096
23		[10.33.7.71]	[10.33.4.53]	Telnet: C PORT=4140 <0D0A>
24		[10.33.4.53]	[10.33.7.71]	Telnet: R PORT=4140 <0D>
25		[10.33.7.71]	[10.33.4.53]	TCP: D=23 S=4140 ACK=2261254731 WIN=17447
26		[10.33.4.53]	[10.33.7.71]	Telnet: R PORT=4140 <0A>Console>
27		[10.33.7.71]	[10.33.4.53]	TCP: D=23 S=4140 ACK=2261254741 WIN=17437
28		[10.33.7.71]	[10.33.4.53]	Telnet: C PORT=4140 e
29		[10.33.4.53]	[10.33.7.71]	Telnet: R PORT=4140 e
30		[10.33.7.71]	[10.33.4.53]	Telnet: C PORT=4140 n
31		[10.33.4.53]	[10.33.7.71]	Telnet: R PORT=4140 n
32		[10.33.7.71]	[10.33.4.53]	TCP: D=23 S=4140 ACK=2261254743 WIN=17435
33		[10.33.7.71]	[10.33.4.53]	Telnet: C PORT=4140 <0D0A>
34		[10.33.4.53]	[10.33.7.71]	Telnet: R PORT=4140 <0D>
35		[10.33.7.71]	[10.33.4.53]	TCP: D=23 S=4140 ACK=2261254744 WIN=17434
36		[10.33.4.53]	[10.33.7.71]	Telnet: R PORT=4140 <0D0A0D0A>Enter password:
37		[10.33.7.71]	[10.33.4.53]	TCP: D=23 S=4140 ACK=2261254764 WIN=17414
38		[10.33.7.71]	[10.33.4.53]	Telnet: C PORT=4140 a
39		[10.33.4.53]	[10.33.7.71]	TCP: D=4140 S=23 ACK=2468036450 WIN=4096
40		[10.33.7.71]	[10.33.4.53]	Telnet: C PORT=4140 z
41		[10.33.4.53]	[10.33.7.71]	TCP: D=4140 S=23 ACK=2468036451 WIN=4096
42		[10.33.7.71]	[10.33.4.53]	Telnet: C PORT=4140 p
43		[10.33.4.53]	[10.33.7.71]	TCP: D=4140 S=23 ACK=2468036452 WIN=4096

Expert Decode Matrix Host Table Protocol Dist. Statistics

For Help, press F1

Visualisation du nom de domaine vtp



38	DIRECTOR1	[10.0.1.255]	NETLOGON: Query for Primary DC	280	0:00:15.960
39	00D0D3D3B28C	Bridge_Group_Ad	BPDU: S: Pri=2000 Port=804D Root: Pri=2000 Add:	60	0:00:16.001
40	[172.16.1.114]	[224.0.0.2]	HSRP: Hello State=Active	62	0:00:16.116
41	00D0D3D3B28C	01000CCCCCCC	DISL: Type=0x0001 (Domain Name)	60	0:00:16.604
42	626D736E626C	010001001062	DISL: Type=0x0001 (Domain Name)	94	0:00:16.605
43	DIRECTOR1	[172.16.53.1]	WINS: C ID=41612 OP=REFRESH NAME=DIRECTOR1<0	110	0:00:16.705
44	#	[172.16.1.114]	Director: ICMP Host Unreachable	70	0:00:16.705
			ICMP: Destination unreachable (Host unreachable)		
45	DIRECTOR1	[10.0.1.255]	WINS: C ID=49532 OP=QUERY NAME=POD1<1C>	92	0:00:16.710
46	DIRECTOR1	[10.0.1.255]	WINS: C ID=49528 OP=QUERY NAME=POD1<1B>	92	0:00:16.710
47	DIRECTOR1	[172.16.53.1]	WINS: C ID=41610 OP=QUERY NAME=POD1<1B>	92	0:00:16.945

DISL:		
DISL: LLC	= 0xAAAA03	
DISL: SNAP Org ID	= 0x00000C (Cisco)	
DISL:		
DISL: HDLC Protocol Type	= 0x2004	
DISL: Version	= 1	
DISL:		
DISL: Message type	= 0x0001 (Domain Name)	
DISL: Message length	= 16	
DISL: Management domain name	= "bcmsnblock1"	
DISL:		
DISL: Message type	= 0x0002 (Status)	
DISL: Message length	= 5	

Les points sensibles : les équipements réseau



- Routeurs et serveurs d'accès : telnet,ssh
- Commande et fonctions
finger, proxy-arp
- protocoles de routage ...



capture de trames suite ...



- capture d'une séquence telnet et password secret pour un routeur
- visualisation d'utilisateurs connectés
- modifications du routage

telnet routeur



Parade SSH
(connexion telnet
sécurisée)

29		[139.4.1.65]	[139.4.1.66]	TCP: D=23 S=13378 ACK=1178996140 WIN=4053
30	#	[139.4.1.66]	[139.4.1.65]	Telnet: C PORT=13378 e Expert: Ack Too Long (202ms)
31		[139.4.1.65]	[139.4.1.66]	TCP: D=13378 S=23 ACK=3396532643 WIN=4081
32		[139.4.1.66]	[139.4.1.65]	Telnet: C PORT=13378 <0D0A>
33		[139.4.1.65]	[139.4.1.66]	Telnet: R PORT=13378 <0D0A>p4-r3>
34		[139.4.1.65]	[139.4.1.66]	TCP: D=23 S=13378 ACK=1178996148 WIN=4045
35		[139.4.1.66]	[139.4.1.65]	Telnet: C PORT=13378 e
36		[139.4.1.65]	[139.4.1.66]	Telnet: R PORT=13378 e
37		[139.4.1.66]	[139.4.1.65]	Telnet: C PORT=13378 n
38		[139.4.1.65]	[139.4.1.66]	Telnet: R PORT=13378 n
39		[139.4.1.65]	[139.4.1.66]	TCP: D=23 S=13378 ACK=1178996150 WIN=4043
40		[139.4.1.66]	[139.4.1.65]	Telnet: C PORT=13378 <0D0A>
41		[139.4.1.66]	[139.4.1.65]	Telnet: R PORT=13378 <0D0A>
42		[139.4.1.65]	[139.4.1.66]	Telnet: R PORT=13378 Password:
43		[139.4.1.65]	[139.4.1.66]	TCP: D=23 S=13378 ACK=1178996162 WIN=4031
44		[139.4.1.66]	[139.4.1.65]	Telnet: C PORT=13378 e
45		[139.4.1.65]	[139.4.1.66]	TCP: D=13378 S=23 ACK=3396532650 WIN=4074
46		[139.4.1.65]	[139.4.1.66]	Telnet: C PORT=13378 x
47		[139.4.1.66]	[139.4.1.65]	Telnet: C PORT=13378 p
48		[139.4.1.65]	[139.4.1.66]	TCP: D=13378 S=23 ACK=3396532652 WIN=4072
49		[139.4.1.65]	[139.4.1.66]	Telnet: C PORT=13378 e
50		[139.4.1.66]	[139.4.1.65]	Telnet: C PORT=13378 r
51		[139.4.1.65]	[139.4.1.66]	TCP: D=13378 S=23 ACK=3396532654 WIN=4070
52		[139.4.1.65]	[139.4.1.66]	Telnet: C PORT=13378 t
53		[139.4.1.66]	[139.4.1.65]	Telnet: C PORT=13378 <0D0A>
54		[139.4.1.66]	[139.4.1.65]	TCP: D=13378 S=23 ACK=3396532657 WIN=4067
55		[139.4.1.65]	[139.4.1.66]	Telnet: R PORT=13378 <0D0A>p4-r3#
56		[139.4.1.65]	[139.4.1.66]	TCP: D=23 S=13378 ACK=1178996170 WIN=4023
57		[139.4.1.65]	[139.4.1.66]	Telnet: C PORT=13378 s

TCP: ----- TCP header -----
 TCP: Source port = 23 (Telnet)

La désactivation de cette fonction sur le routeur, aide a la sécurisation du réseau.

```
C:\WINNT\System32\cmd.exe
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>finger -l @172.16.1.1
[172.16.1.1]
> Finger: connect::Impossible de joindre l'hôte.
C:\>
```

Démo table de routage, sans authentification



```
12 [10.33.97.101] [10.33.97.102] OSPF: Database Description ID=[1.1.1.1]
13 [10.33.97.101] [224.0.0.5] OSPF: Link State Update ID=[1.1.1.1]
14 [10.33.97.102] [10.33.97.101] OSPF: Link State Update ID=[2.2.2.2]
15 [10.33.97.102] [224.0.0.5] OSPF: Link State Update ID=[2.2.2.2]
16 [10.33.97.102] [224.0.0.5] OSPF: Link State Update ID=[2.2.2.2]
17 [10.33.97.101] [224.0.0.5] OSPF: Link State Acknowledgment ID=[1.1.1.1]
18 [10.33.97.101] [10.33.97.102] OSPF: Link State Request ID=[1.1.1.1]
19 [10.33.97.101] [10.33.97.102] OSPF: Link State Update ID=[1.1.1.1]
20 [10.33.97.102] [10.33.97.101] OSPF: Link State Update ID=[2.2.2.2]
21 [10.33.97.102] [10.33.97.101] OSPF: Link State Update ID=[2.2.2.2]
22 [10.33.97.101] [224.0.0.5] OSPF: Link State Update ID=[1.1.1.1]
```



```
IP: Source address      = [10.33.97.102]
IP: Destination address = [224.0.0.5]
IP: No options
IP:
OSPF: ----- OSPF Header -----
OSPF:
OSPF: Version = 2,      Type = 1 (Hello),    Length = 44
OSPF: Router ID       = [2.2.2.2]
OSPF: Area ID         = [0.0.0.0]
OSPF: Header checksum = 9013 (correct)
OSPF: Authentication: Type = 0 (No Authentication), Value = 00 00 00 00 00 00 00 00
OSPF:
OSPF: Network mask     = [255.255.252.0]
```

capture des infos sur protocoles de routage
injection de mauvaises routes, plus protection des échanges
par password chiffrés et signés

Table de Routage suite ... avec authentification



```
32 [10.33.97.101] [224.0.0.5] OSPF: Hello ID=[1.1.1.1]
33 [10.33.97.102] [224.0.0.5] OSPF: Hello ID=[2.2.2.2]
34 [10.33.97.101] [224.0.0.5] OSPF: Hello ID=[1.1.1.1]
35 [10.33.97.102] [224.0.0.5] OSPF: Hello ID=[2.2.2.2]
36 [10.33.97.101] [224.0.0.5] OSPF: Hello ID=[1.1.1.1]
37 [10.33.97.102] [224.0.0.5] OSPF: Hello ID=[2.2.2.2]
38 [10.33.97.101] [224.0.0.5] OSPF: Hello ID=[1.1.1.1]
39 [10.33.97.102] [224.0.0.5] OSPF: Hello ID=[2.2.2.2]
40 [10.33.97.102] [224.0.0.5] OSPF: Link State Update ID=[2.2.2.2]
41 [10.33.97.101] [224.0.0.5] OSPF: Hello ID=[1.1.1.1]
42 [10.33.97.101] [224.0.0.5] OSPF: Link State Acknowledgment ID=[1.1.1.1]
43 [10.33.97.102] [224.0.0.5] OSPF: Hello ID=[2.2.2.2]
44 [10.33.97.101] [224.0.0.5] OSPF: Hello ID=[1.1.1.1]
45 [10.33.97.102] [224.0.0.5] OSPF: Hello ID=[2.2.2.2]
```

```
OSPF: ----- OSPF Header -----
OSPF:
OSPF: Version = 2,   Type = 1 (Hello),   Length = 48
OSPF: Router ID      = [1.1.1.1]
OSPF: Area ID        = [0.0.0.0]
OSPF: Header checksum = 0000 (correct)
OSPF: Authentication: Type = 2 (Reserved type),   Value = 00 30 01 10 00 00 00 2D
OSPF:
```

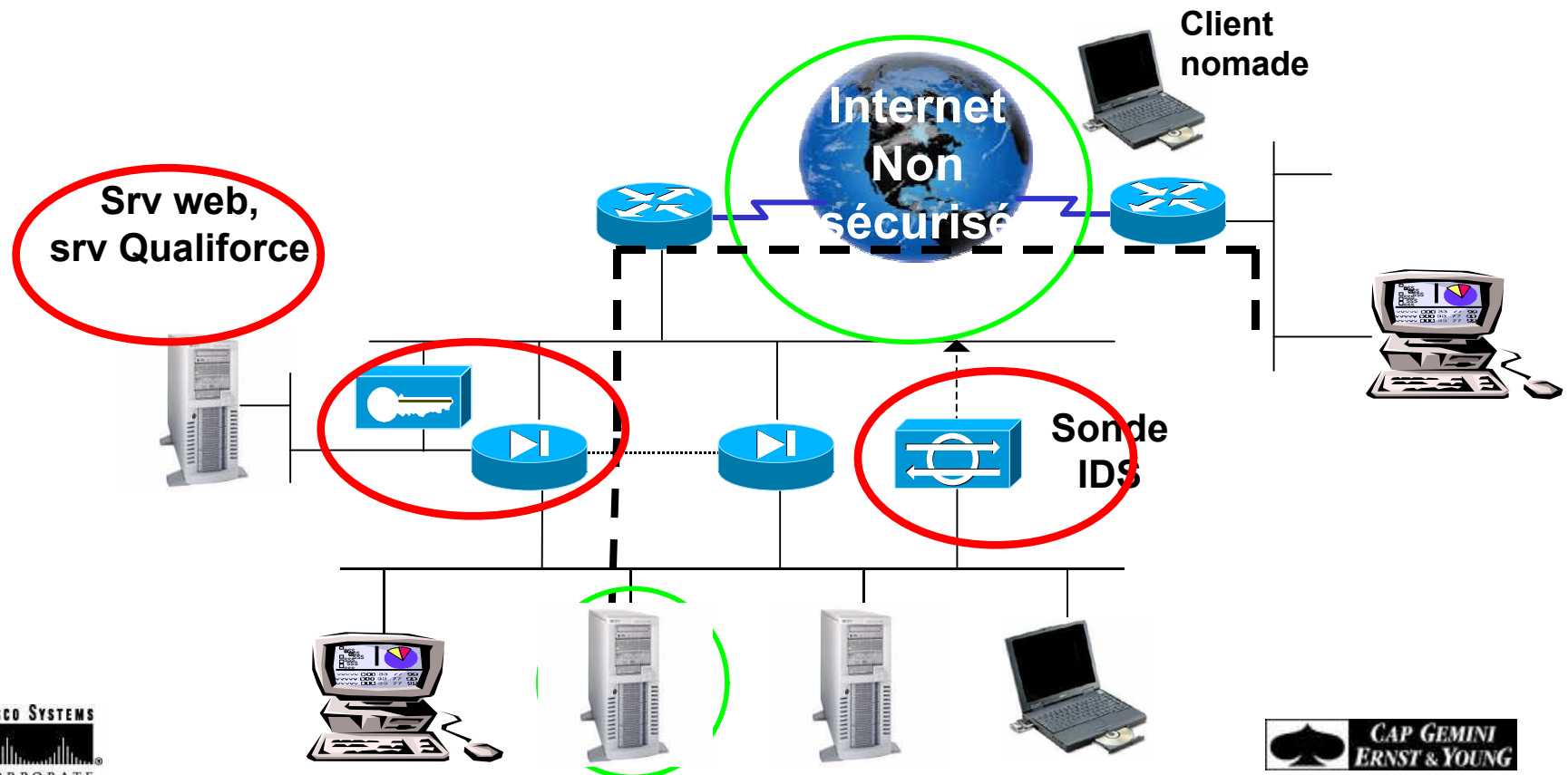
Afin d'éviter tout problème, d'injection de routes, il faut absolument activer l'authentification, et la définition du voisinage au niveau des protocoles de routage.

La capture de trafic ...



Dans un certain nombre de cas, la capture de trafic afin de récupérer des infos ou des données confidentielles, est IMPARABLE.

C'est pourquoi la mise en œuvre de canaux vpn devient indispensable, sur le lan, aussi bien que dans l'interconnexion de sites, ou dans le cas de clients nomades.



Trafic non chiffré



```

82 [139.4.1.66] [139.4.1.65] Telnet: R PORT=13378 <0D0A>
83 [139.4.1.65] [139.4.1.66] TCP: D=23 S=13378 ACK=1178996183 WIN=4010
84 [139.4.1.66] [139.4.1.65] Telnet: R PORT=13378 Codes: C - connected, S - static, I -
85 [139.4.1.66] [139.4.1.65] Telnet: R PORT=13378 variably subnetted, 11 subnets, 6 me
86 [139.4.1.65] [139.4.1.66] TCP: D=23 S=13378 ACK=1178997303 WIN=2890
87 [139.4.1.66] [139.4.1.65] Telnet: R PORT=13378 connected, Loopback0<0D0A>C 139
88 [139.4.1.65] [139.4.1.66] TCP: D=23 S=13378 ACK=1178997863 WIN=4128
89 [139.4.1.66] [139.4.1.65] Telnet: R PORT=13378 .65, 00:24:42, Ethernet0<0D0A>S 20
90 [139.4.1.65] [139.4.1.66] TCP: D=23 S=13378 ACK=1178998089 WIN=3902
91 [139.4.1.65] [139.4.1.66] Telnet: C PORT=13378 e
92 [139.4.1.66] [139.4.1.65] Telnet: R PORT=13378 e
93 [139.4.1.65] [139.4.1.66] Telnet: C PORT=13378 x
94 [139.4.1.66] [139.4.1.65] Telnet: R PORT=13378 x
95 [139.4.1.65] [139.4.1.66] Telnet: C PORT=13378 i

```

```

TCP:
Telnet: ----- Telnet -----
Telnet:
Telnet: .65, 00:24:42, Ethernet0<0D0A>S 207.4.96.0/19 [1/0] via 139.4.2.2<0D0A>B...
Telnet:

```

```

00000000: 00 10 7b 04 a3 61 00 e0 1e b9 99 56 08 00 45 c0 ...{.fa.à.'IV..EÀ
00000010: 01 0a 00 22 00 00 ff 06 a1 80 8b 04 01 42 8b 04 ...".ÿ.!!!..B!
00000020: 01 41 00 17 34 42 46 46 14 67 ca 72 f9 be 50 18 .A..4BFF.gËrûMP.
00000030: 0f d6 fe c0 00 00 2e 36 35 2c 20 30 30 3a 32 34 .OpÀ...65, 00:24
00000040: 3a 34 32 2c 20 45 74 68 65 72 6e 65 74 30 0d 0a .42, Ethernet0..
00000050: 53 20 20 20 20 32 30 37 2e 34 2e 39 36 2e 30 2f S 207.4.96.0/
00000060: 31 39 20 5b 31 2f 30 5d 20 76 69 61 20 31 33 39 19 [1/0] via 139
00000070: 2e 34 2e 32 2e 32 0d 0a 42 20 20 20 20 32 30 33 .4.2.2..B 203
00000080: 2e 34 2e 30 2e 30 2f 31 36 20 5b 32 30 2f 30 5d .4.0.0/16 [20/0]
00000090: 20 76 69 61 20 31 33 39 2e 34 2e 32 2e 32 2c 20 via 139.4.2.2,
000000a0: 30 30 3a 32 33 3a 33 35 0d 0a 53 20 20 20 20 32 00:23:35..S 2
000000b0: 30 37 2e 34 2e 36 34 2e 30 2f 31 39 20 5b 31 2f 07.4.64.0/19 [1/
000000c0: 30 5d 20 76 69 61 20 31 33 39 2e 34 2e 32 2e 32 0] via 139.4.2.2
000000d0: 0d 0a 4f 20 45 32 20 31 35 30 2e 30 2e 30 2e 30 .O E2 150.0.0.0

```

Show ip route en trafic non chiffré

Trafic chiffré - VPN IPSEC -



52	[139.4.1.66]	[139.4.1.65]	IP: ESP SPI=31459046
53	[139.4.1.65]	[139.4.1.66]	IP: ESP SPI=30677379
54	[139.4.1.66]	[139.4.1.65]	IP: ESP SPI=31459046
55	[139.4.1.65]	[139.4.1.66]	IP: ESP SPI=30677379
56	[139.4.1.65]	[139.4.1.66]	IP: ESP SPI=30677379
57	[139.4.1.66]	[139.4.1.65]	IP: ESP SPI=31459046
58	[139.4.1.65]	[139.4.1.66]	IP: ESP SPI=30677379
59	[139.4.1.65]	[139.4.1.66]	IP: ESP SPI=30677379
60	[139.4.1.66]	[139.4.1.65]	IP: ESP SPI=31459046

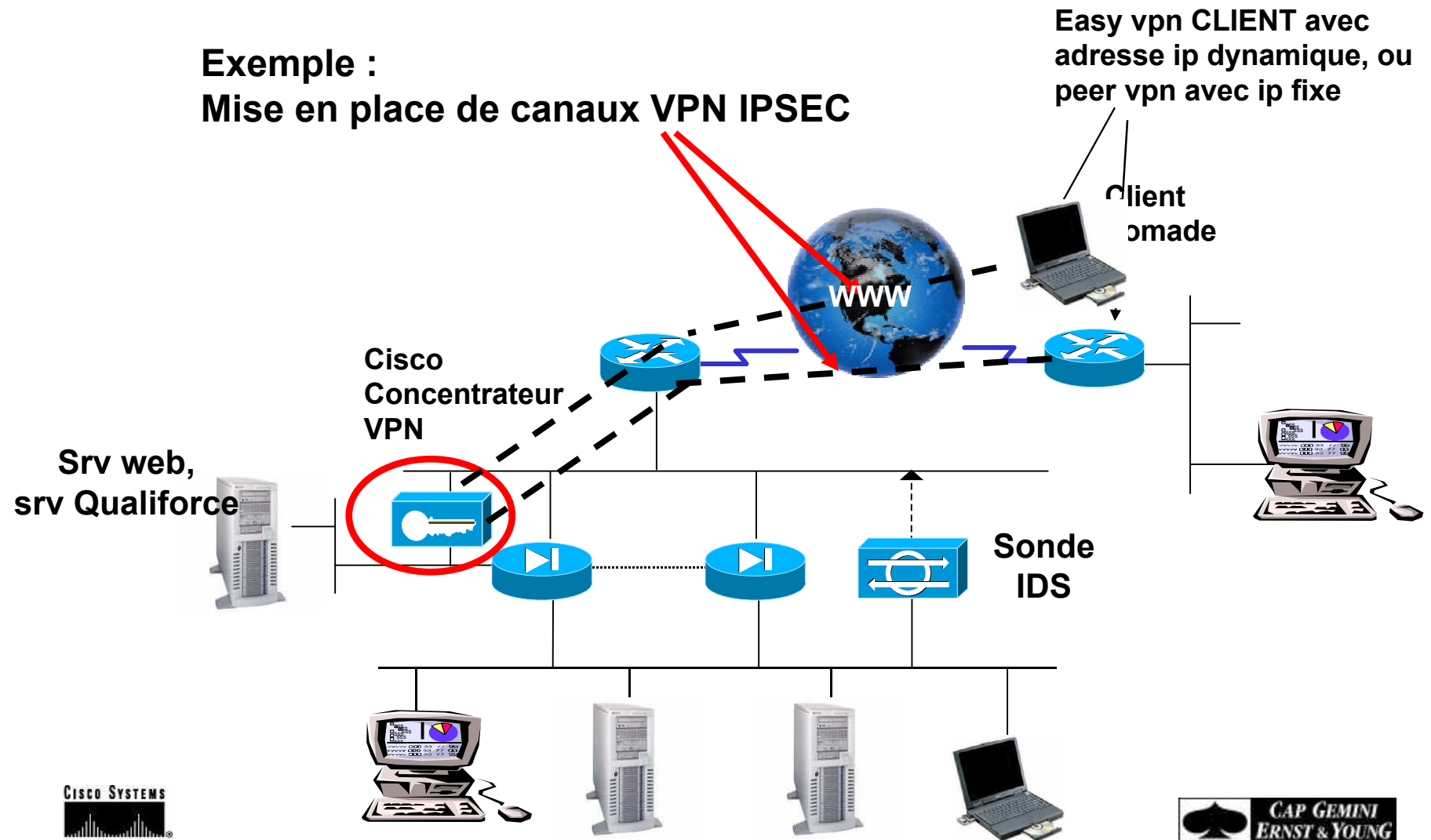
IP:	No options
IP:	
ESP:	----- IP ESP -----
ESP:	
ESP:	Security Parameters Index = 30677379
ESP:	Sequence Number = 21
ESP:	Payload Data = A002C941C5A6BDD0EBEC8EA7DB0393A4DBD5A235BE9D424B28C141CFE76F597323067B9A1B49

00000000:	00 e0 1e b9 99 56 00 10 7b 04 a3 61 08 00 45 c0	.à.¹ V..{.fa..EÀ
00000010:	00 54 9e 72 00 00 ff 32 03 ba 8b 04 01 41 8b 04	.Tr...ÿ2.º...À
00000020:	01 42 01 d4 19 83 00 00 00 15 a0 02 c9 41 c5 a6	.B.Ö.EAA
00000030:	bd d0 eb ec 8e a7 db 03 93 a4 db d5 a2 35 be 9d	%Dei SÜ. µÜc5%
00000040:	42 4b 28 c1 41 cf e7 6f 59 73 23 06 7b 9a 1b 49	BK(ÁAİçoYs#.{ .I
00000050:	35 c0 49 46 52 17 60 fd 86 20 2d 7e a2 e2 1f ef	5AİFR.´ý -~câ.İ
00000060:	25 7d	%}

Canaux VPN IPSEC



**Exemple :
Mise en place de canaux VPN IPSEC**



Démo 4 VPN IPSEC



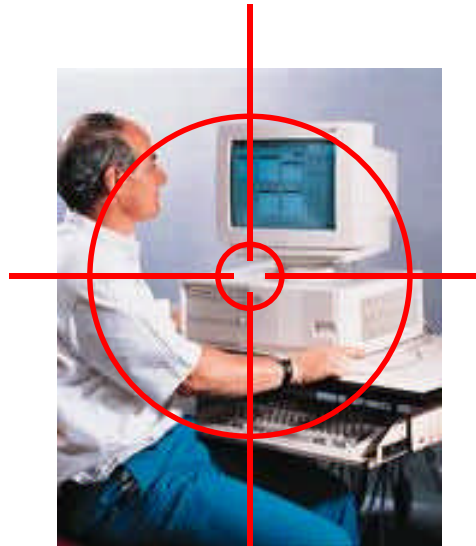
**Demo – connexion vpn ipsec nomade
Client nomade Canal VPN IPSEC 3 des / ou AES
vers le concentrateur vpn**

Les points sensibles : Les utilisateurs



**La Sensibilisation des utilisateurs à la sécurité est
primordiale, dans une politique de sécurité cohérente**

**Les meilleures protections restent totalement
inopérantes dans le cas du Social Engineering**



**Les points sensibles :
Les utilisateurs suite ...**



ANALYSE D'UNE ATTAQUE BASEE SUR UNE DEMANDE A L'UTILISATEUR

**- Voici quelque chose de ravageur dans le milieu du hacking
Ce processus assez simple a mettre en place est basé sur une demande de
renseignements directement a l'utilisateur :**

ETAPE n°1:

**Creation d'un Script php : envoi d'un mail a des utilisateurs en se faisant passer pour
l'administrateur du site, avec demande de nom et mot de passe.**

ETAPE n°2

**Creation d'un second script pour demander toutes les informations a l'utilisateur via une page
html et renvoyer ces réponses vers un lien url interne ou externe mais l'utilisateur n'en sait rien**



Pendant l'attaque



4

Et en Continu

Remontées d'Alertes

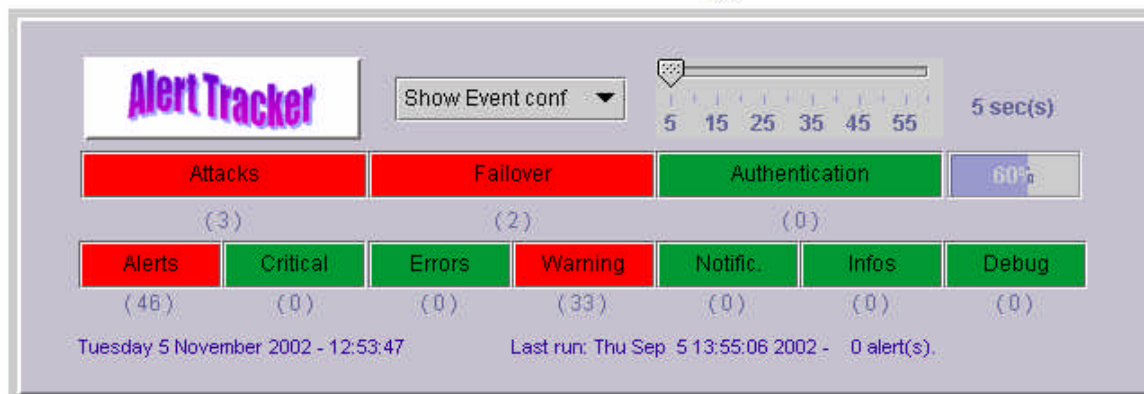


Attaques externes : Détection et notification des alertes critiques par Qualiforce



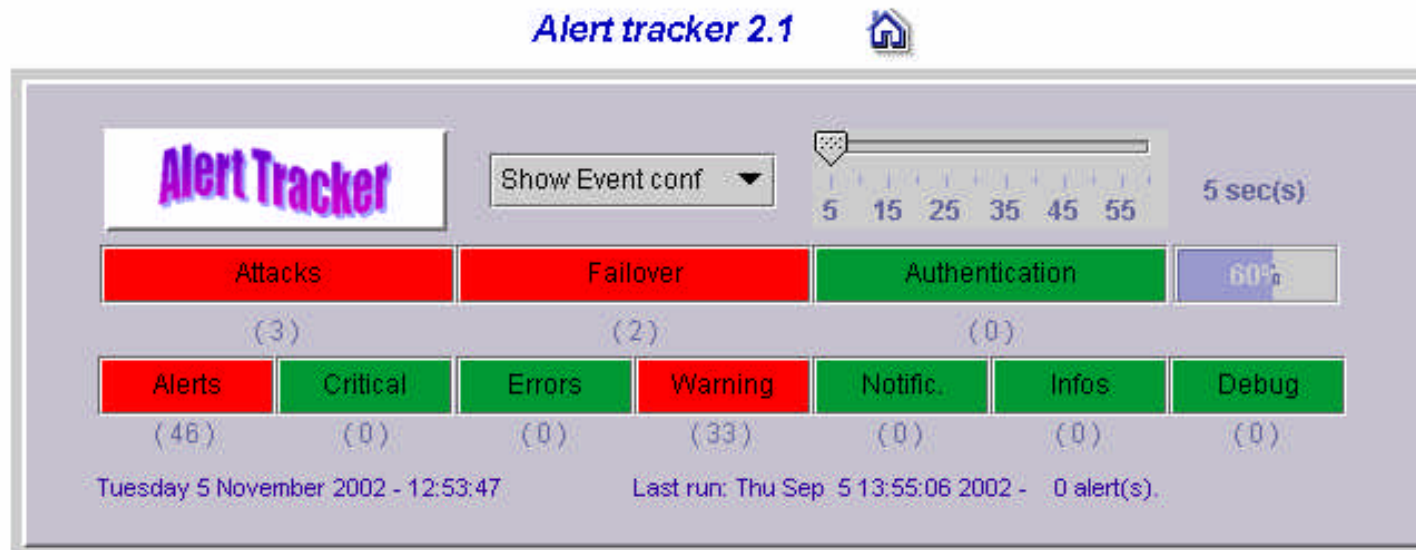
PIX 501,506, 515, ...

Alert tracker 2.1 



```
%8%PIX-4-400033: IDS:4052 UDP Chargen DoS attack
%8%PIX-4-400034: IDS:6050 DNS HINFO Request
%8%PIX-4-400035: IDS:6051 DNS Zone Transfer
%8%PIX-4-400036: IDS:6052 DNS Zone Transfer from High Port
%8%PIX-4-400037: IDS:6053 DNS Request for All Records
%8%PIX-4-400041: IDS:6103 Proxied RPC Request
%8%PIX-4-400050: IDS:6190 statd Buffer Overflow
%8%PIX-4-400051: IDS:8000 FTP Retrieve Password File
#
#
## Critical level Attack messages
%8%PIX-2-106016: Deny IP spoof from
%8%PIX-2-106017: Deny IP due to Land Attack from
%10%PIX-2-109006: Authentication failed for user
#
#
## Severity 1 (Alert Messages)
%9%PIX-1-101001: (Primary) Failover cable OK
%9%PIX-1-101001: (Secondary) Failover cable OK
%9%PIX-1-101002: (Primary) Bad failover cable
```

Mon PIX Fail Over a-t-il basculé ? Détection et alerte par Qualiforce (1/2)



Failover category events [Clear alerts](#)

Sep 05 13:17:37 192.168.1.220 Nov 05 2002 11:15:56: %PIX-1-105007: (Secondary) Link status 'Down' on interface 5
Sep 05 13:17:42 192.168.1.220 Nov 05 2002 11:16:01: %PIX-1-102001: (Secondary) Power failure/System reload other side.

Mon PIX Fail Over a-t-il basculé ? Détection et alerte par Qualiforce (2/2)



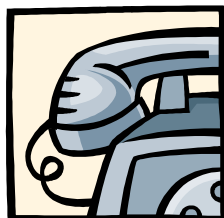
Par **MAIL**

From: <PIX_ALERT@qualiforce.fr>
To: <jean-pierre.regina@qualiforce.fr>
Sent: Thursday, September 05, 2002 12:18 PM
Subject: Alert Tracker PIX alarm !!

Sep 05 13:17:37 192.168.1.220 Nov 05 2002 11:15:56: %PIX-1-105007: (Secondary) Link status 'Down' on interface 5

Sep 05 13:17:42 192.168.1.220 Nov 05 2002 11:16:01: %PIX-1-102001: (Secondary) Power failure/System reload other side.

Par



ou

SMS



Alert Tracker - Log Report



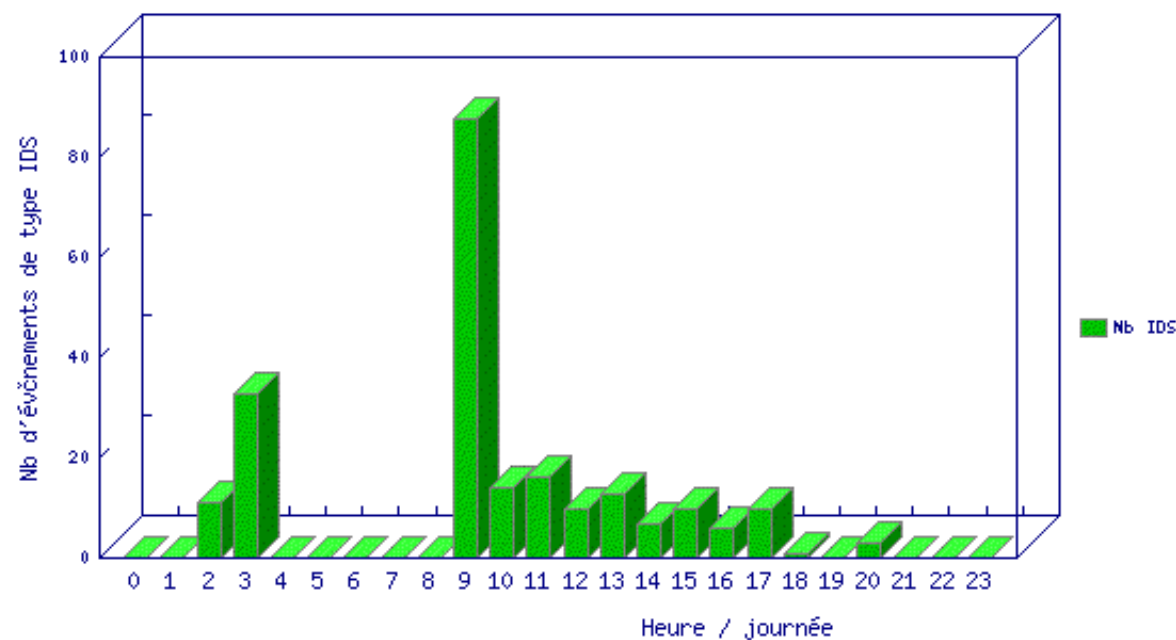
Blocage de l'attaque par le PIX et Remontée d'alertes par Qualiforce



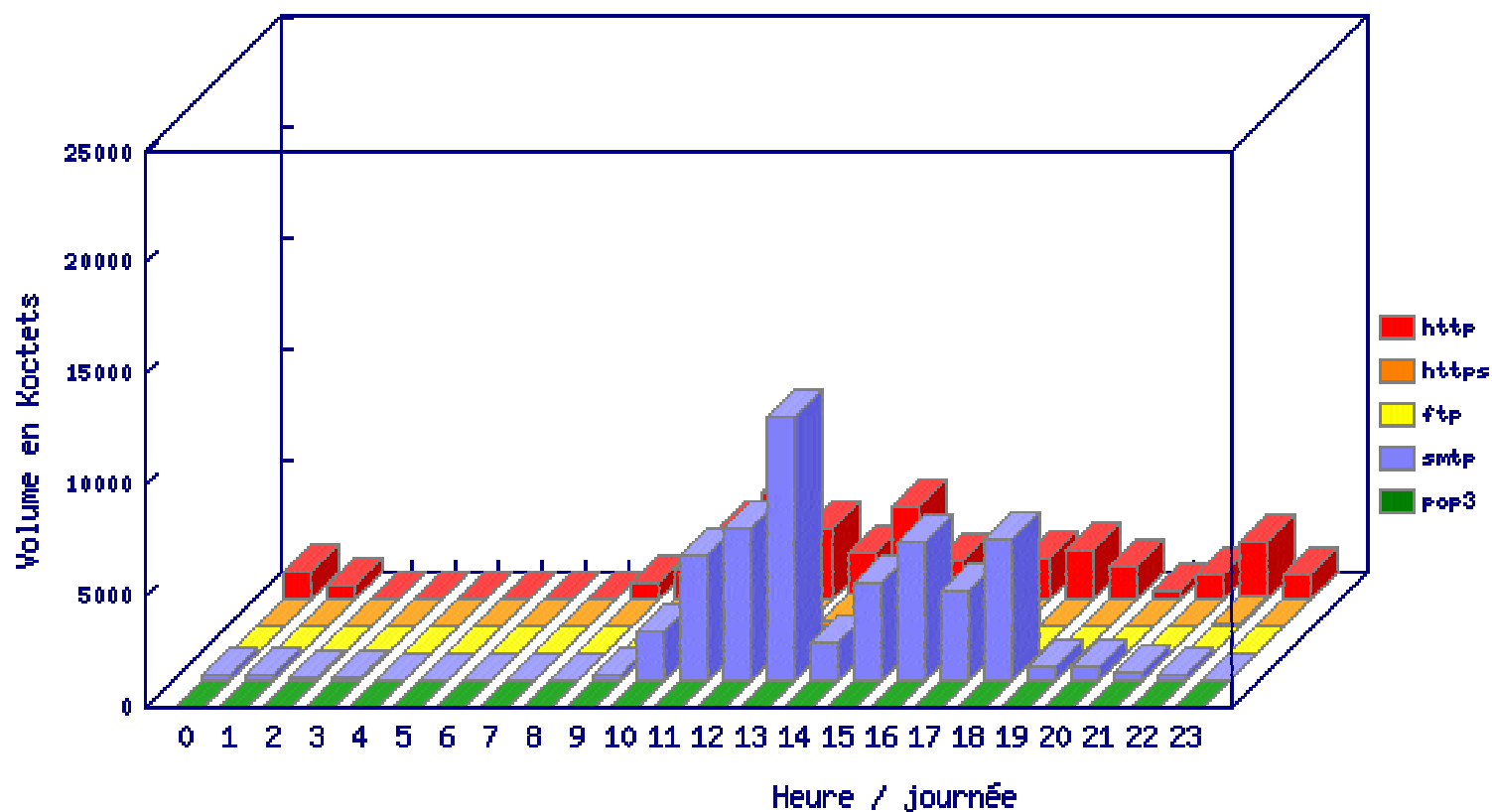
8) Evènements IDS par tranche horaire



Cette section synthétise le nombre d'évènements de type "IDS" (Intrusion Detection System) détectés par tranche horaire, sur la période de référence.



Visualisation des statistiques PIX avec Qualiforce

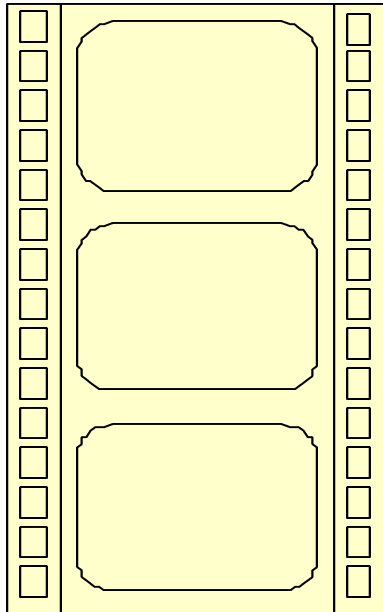




Cisco Secure Tour 4



- **DEMONSTRATION !!**



- **Remontée d'Alerte par Qualiforce**



Après l'attaque



3

Correctif

Contrôle d'Intégrité

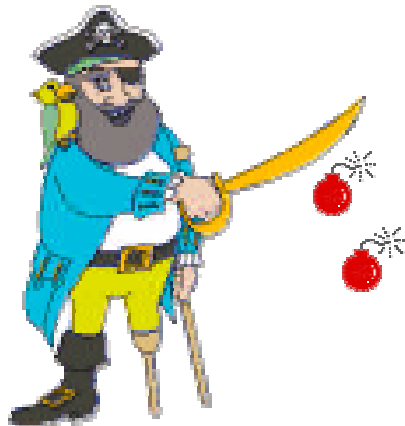
Contrôle d'Intégrité
~~TRIPWIRE~~
TRIPWIRE



Mise en Situation de l'exploitation



Tous les systèmes sont sensibles à une attaque interne ou externe



- Unix
- Windows



O.S Propriétaire

Bénéfices d'une Surveillance



Tripwire est une gamme de logiciels qui vous permet de détecter automatiquement les modifications et d'alerter les administrateurs.



- SNMP
- MAIL
- SYSLOG
- Tripwire Manager



- Fichiers
- Répertoires
- Base de Registre



O.S Propriétaire

Bénéfices d'une Surveillance

Tripwire Manager: Rapport



- Descriptif **exact** de ce qui est touché.

Tripwire Manager -> Controller

File Edit Manager Machine View Help

Report Viewer

Violations Reports Summary Objects

localhost

Windows NT File System

test

c:\temp\Nouveau

Details of c:\temp\Nouveau\Document.txt

Attribute	Expected Value	Observed Value
Compression	0	0
Offline Flag	0	0
Temporary Flag	0	0
Size	0	0
MS-DOS Name	NOUVEAU-1.TXT	NOUVEAU-1.TXT
SD Size	100	100
SD Control	8004	8004
SHA	DA38A3EE5E6B4B0D3255BFF95601800AFD80709	DA38A3EE5E6B4B0D3255BFF95601800AFD80709
HAVAL	1BDC556B2AD02EC08AF8C66477F2A87	1BDC556B2AD02EC08AF8C66477F2A87
MD5	D41D8CD98F00B204E9800998ECF8427E	D41D8CD98F00B204E9800998ECF8427E
CRC32	FFFFFFFF	FFFFFFFF
Num of Alt Streams	0	1
Stream SHA		62479E7497BF3408E8AD7F80F9D729CE9C0632A7
Stream HAVAL		892F32C9E8BEEB9D4D4748A579CA8D6A
Stream MD5		5DB8E27336BAD34DD69C2A34285E778A
Stream CRC32		A61962E0
Access Time	vendredi 11 octobre 2002 11:11:13	vendredi 11 octobre 2002 11:16:00
Write Time	vendredi 11 octobre 2002 11:11:13	vendredi 11 octobre 2002 11:16:00
Create Time	vendredi 11 octobre 2002 11:11:13	vendredi 11 octobre 2002 11:11:13
Owner	COMPUTERLINKS\bertrand	COMPUTERLINKS\bertrand
Group	Unknown	Unknown
DAACL	Revision 2, Size: 112, Number of ACEs: 4 Allow: BUILTIN\Administrateurs Mask: 0x00101ff Flags: None Allow: AUTORITE NTSYSTEM Mask: 0x00101ff Flags: None Allow: COMPUTERLINKS\bertrand Mask: 0x00101ff Flags: None Allow: BUILTIN\Utilisateurs Mask: 0x001200a9 Flags: None	Revision 2, Size: 112, Number of ACEs: 4 Allow: BUILTIN\Administrateurs Mask: 0x00101ff Flags: None Allow: AUTORITE NTSYSTEM Mask: 0x00101ff Flags: None Allow: COMPUTERLINKS\bertrand Mask: 0x00101ff Flags: None Allow: BUILTIN\Utilisateurs Mask: 0x001200a9 Flags: None
SAACL	Null	Null

1 Reports, 1 Violations, Max Severity 50

Filter on

Bénéfices d'une Surveillance

Tripwire: Granularité de la surveillance



Le fichier de politiques permet de définir **exactement** ce que l'on souhaite surveiller

- Sévérité
- Réponse
- Objet
- Récursivité

```
#####  
#  
#####  
# Network Configuration files #  
#  
#####  
(  
  rulename = "Network Configuration files",  
  severity = $(SIG_HIGH),  
  emailto = $(SIG_HIGH_MAILRECIPIENTS),  
  recurse = true  
)  
  
# POSIX Network configuration files  
$(SYSTEM32DRIVERS\etc\hosts -> $(SEC_HIGH);  
$(SYSTEM32DRIVERS\etc\networks -> $(SEC_HIGH);  
$(SYSTEM32DRIVERS\etc\protocols -> $(SEC_HIGH);  
$(SYSTEM32DRIVERS\etc\sensires -> $(SEC_HIGH);  
# Not installed by default, but you may use this if you rename the hosts.sam file  
#$(SYSTEM32DRIVERS\etc\hosts -> $(SEC_HIGH);  
$(SYSTEM32DRIVER\config -> $(SEC_HIGH);  
$(SYSTEM32DRIVER\dhcp -> $(SEC_HIGH);  
$(SYSTEM32DRIVER\iras -> $(SEC_HIGH);  
#$(SYSTEM32DRIVER\ios2 -> $(SEC_HIGH); # Might not be present on system  
$(SYSTEM32DRIVER\isabup -> $(SEC_HIGH);  
$(SYSTEM32DRIVER\shelied -> $(SEC_HIGH);  
$(SYSTEM32DRIVER\wins -> $(SEC_HIGH);  
$(SYSTEMROOT)\security -> $(SEC_HIGH);  
  
# Other files to watch that are not installed by default or are legacy files  
#$(SYSTEM32DRIVER\propl -> $(SEC_HIGH);  
#$(SYSTEMROOT)\Registration -> $(SEC_HIGH);  
)  
  
#####  
#  
#####
```

Bénéfices d'une Surveillance Tripwire



Tripwire est une gamme complète d'outils de sécurité permettant de détecter toutes modifications, tant sur des systèmes que sur des périphériques réseaux

Gamme Système:

- **Tripwire for Servers**
- **Tripwire Manager**

Gamme Réseau:

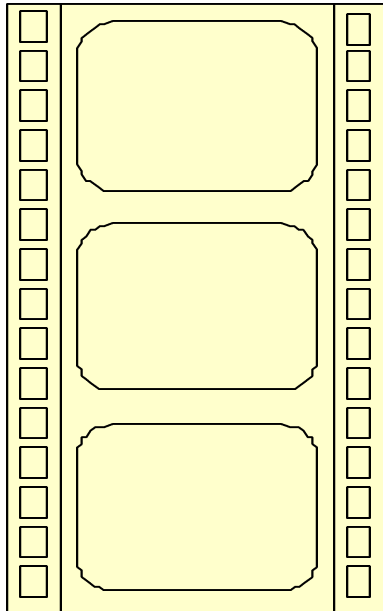
- **Tripwire for Network Devices**

Plus de détails cet après-midi avec:

Rafik Hajem
Directeur - France



- **DEMONSTRATION !!**



- **Intégrité d'un serveur**

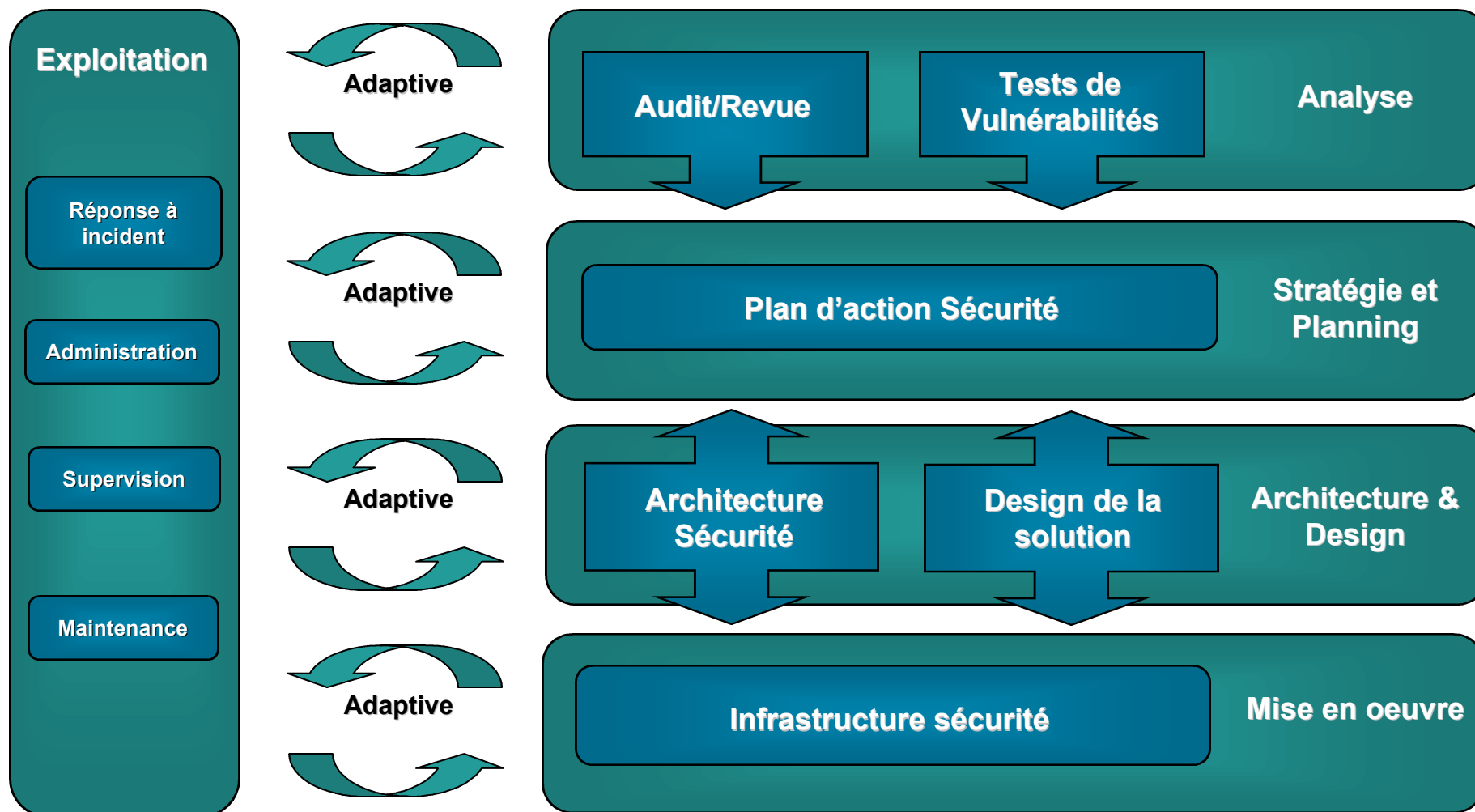


En résumé,



- **Les menaces sont réelles et vont augmenter.**
- **La Sécurité doit être intégrée avec l'infrastructure réseau: ni produits isolés, ni une sécurité ajoutée.**
- **La Sécurité doit être pensée et construite dans chaque élément du réseau.**
- **Évolutivité et Management.**
- **Une Sécurité de bout en bout à travers l'intégration pré-validée de différentes technologies et vendeurs (EcoSystème)**
- **La Roue de Sécurité : pas simplement des produits, mais un processus récurrent**

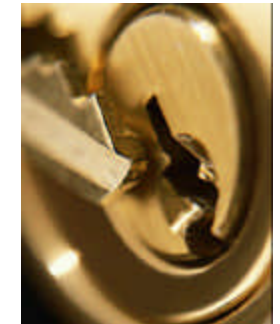
Cette identification des menaces, ce calcul des risques s'inscrit dans un processus sécurité



En Conclusion,



- A vous de déterminer VOS risques, et VOTRE sécurité !!!
 - Quelle sont les menaces principales ?
 - Quelle technologie réseau, applicative, si elle est mise en panne, **ARRETERA** votre activité ?
 - Mettez-vous en place de la sécurité au bon endroit pour les bonnes raisons ?
 - Avez-vous validé les aspects juridiques ?



La sécurité commence par vous !



**Pensez Adaptive Security
dans un EcoSystème Intégré !**



Merci de votre attention !

Ludwig Haché
Cap Gemini Ernst&Young
ludwig.hache@cgey.com

