

Integración de los sistemas IPS en un entorno Wifi centralizado



Marcos Jimena – Cisco

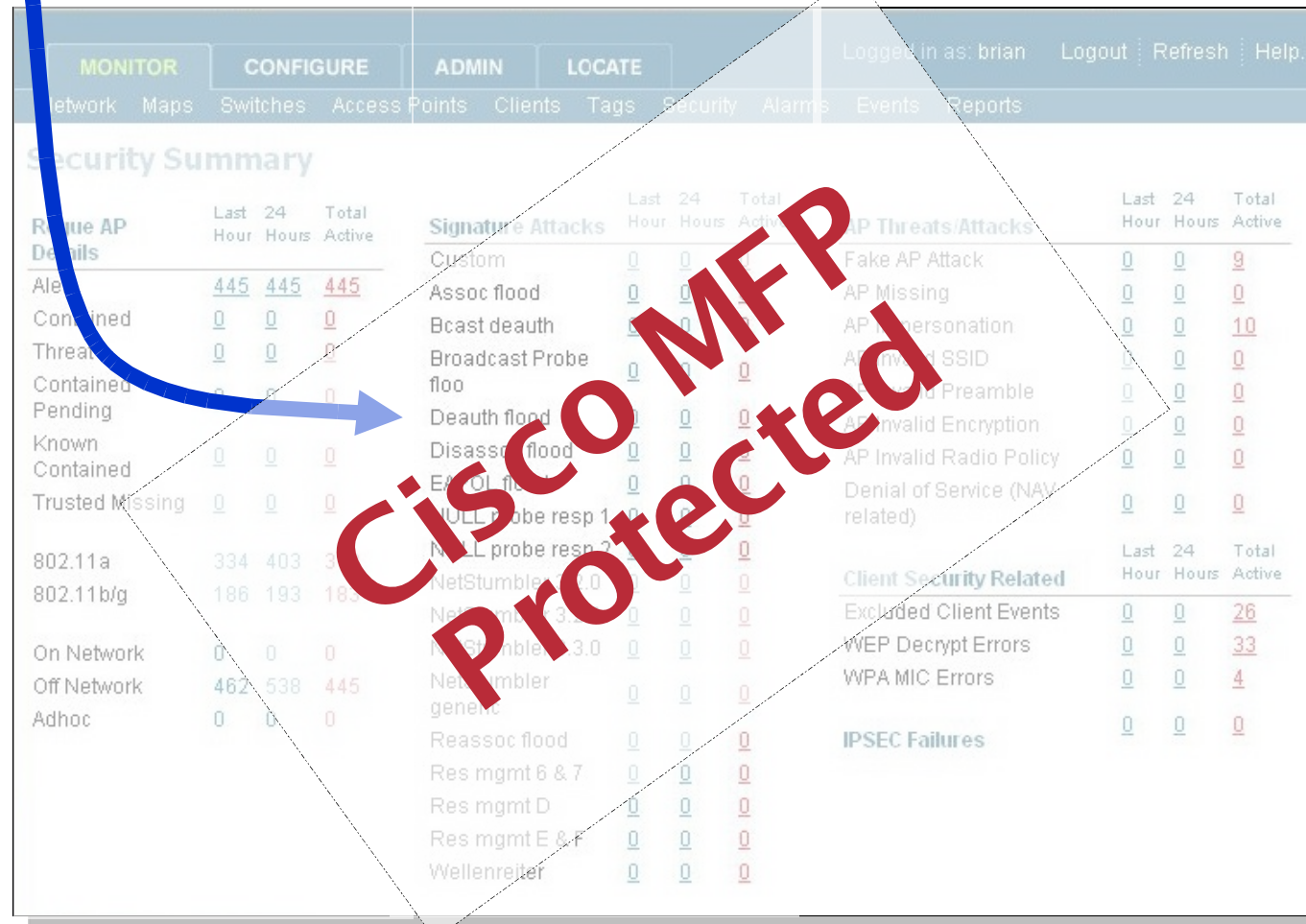
Abril 2007

¿Qué tipo de ataques hacen vulnerable a 802.11?

Most common attacks are against management frames

Ataques comunes:

- VOID11
- Aireplay
- File2air
- Airforge
- ASLEAP
- Jack attacks
- FakeAP
- Hunter/Killer



The screenshot shows the Cisco MFP Security Summary dashboard. A large red watermark 'Cisco MFP Protected' is overlaid diagonally across the center. A blue arrow points from the left side of the slide to the 'Signature Attacks' table in the dashboard.

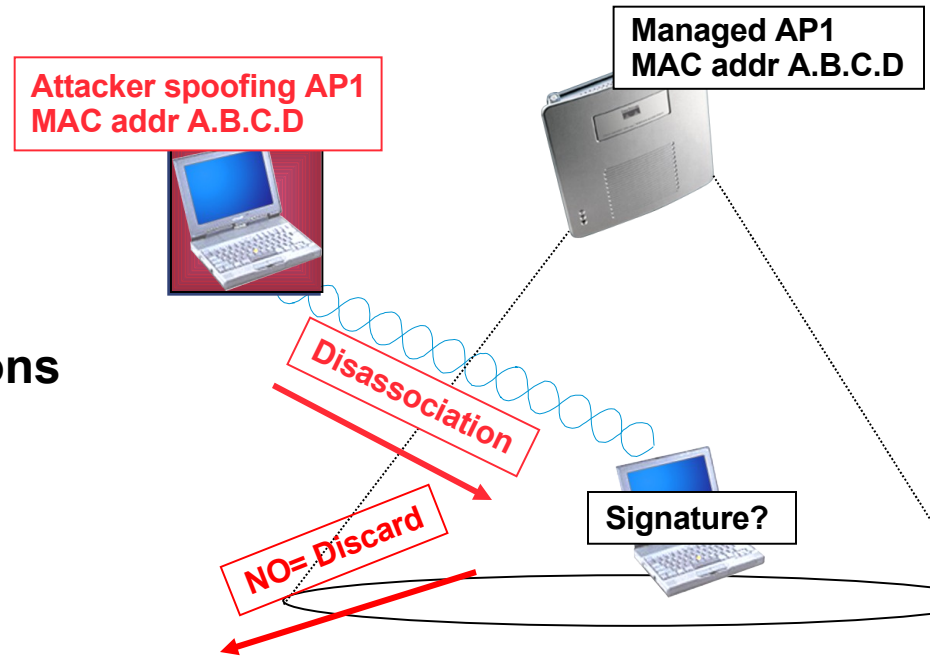
MONITOR				CONFIGURE				ADMIN				LOCATE				Logged In as: brian Logout Refresh Help																							
Network				Maps				Switches				Access Points				Clients				Tags				Security				Alarms				Events				Reports			
Security Summary																																							
 Rogue AP Details												 Signature Attacks												 AP Threats/Attacks															
		Last Hour	24 Hours	Total Active			Last Hour	24 Hours	Total Active			Last Hour	24 Hours	Total Active			Last Hour	24 Hours	Total Active			Last Hour	24 Hours	Total Active			Last Hour	24 Hours	Total Active										
Alerts		445	445	445	Custom		0	0	0	Fake AP Attack		0	0	0	AP Missing		0	0	0	AP impersonation		0	0	10	AP Invalid SSID		0	0	0										
Contained		0	0	0	Bcast death		0	0	0	AP Invalid Preamble		0	0	0	AP Invalid Encryption		0	0	0	Denial of Service (NAV related)		0	0	0	Client Security Related														
Threats		0	0	0	Broadcast Probe flood		0	0	0	AP Invalid Radio Policy		0	0	0	Excluded Client Events		0	0	26	WEP Decrypt Errors		0	0	33	WPA MIC Errors		0	0	4										
Contained Pending		0	0	0	Death flood		0	0	0	Denial of Service (NAV related)		0	0	0	IPSEC Failures		0	0	0																				
Known		0	0	0	Disassoc flood		0	0	0																														
Contained		0	0	0	EAPOL flood		0	0	0																														
Trusted Missing		0	0	0	NULL probe resp 1		0	0	0																														
802.11a		334	403	334	NULL probe resp 2		0	0	0																														
802.11b/g		186	193	186	NetStumble 1.0		0	0	0																														
On Network		0	0	0	NetStumble 3.0		0	0	0																														
Off Network		462	538	445	NetStumble 3.0		0	0	0																														
Adhoc		0	0	0	NetStumble generic		0	0	0																														
					Reassoc flood		0	0	0																														
					Res mgmt 6 & 7		0	0	0																														
					Res mgmt D		0	0	0																														
					Res mgmt E & F		0	0	0																														
					Wellenreiter		0	0	0																														

Management Frame Protection (MFP)

Problema: No hay “seguridad física” para wireless y tramas de gestión, que no están ni autenticadas, ni cifradas ni firmadas

Solución: Insertar una firma digital (MIC) en las tramas de gestión

- AP beacons
- Probe Requests/Responses
- Associations/Re-associations
- Disassociations
- Authentications/De-authentications
- Action Management Frames



•Si las Tramas de Gestión no tienen la firma correcta, tanto la infraestructura como los clientes podrán descartar dicha trama

WIDS 802.11 Signature Analysis

- **Potentially service-impacting 802.11 (or non-802.11) traffic should be characterized/detected**

Interference (white noise, Bluetooth, legacy 802.11, or other ISM-band interferers)

Denial of Service exploits (association, probe, EAP)

Reconnaissance tools (Netstumbler, etc.)

Exploit tools (Monkey-Jack, FakeAP, etc.)

- **Note that 802.11 Management Frames—association/authentication probe are not encrypted or authenticated in current implementation**

Thus, it is not possible to eliminate the possibility of Denial of Service attacks

The severity of such DoS events should be characterized

Mechanisms for securing 802.11 control messages are being considered, but will induce compatibility challenges

WIDS Signature Analysis

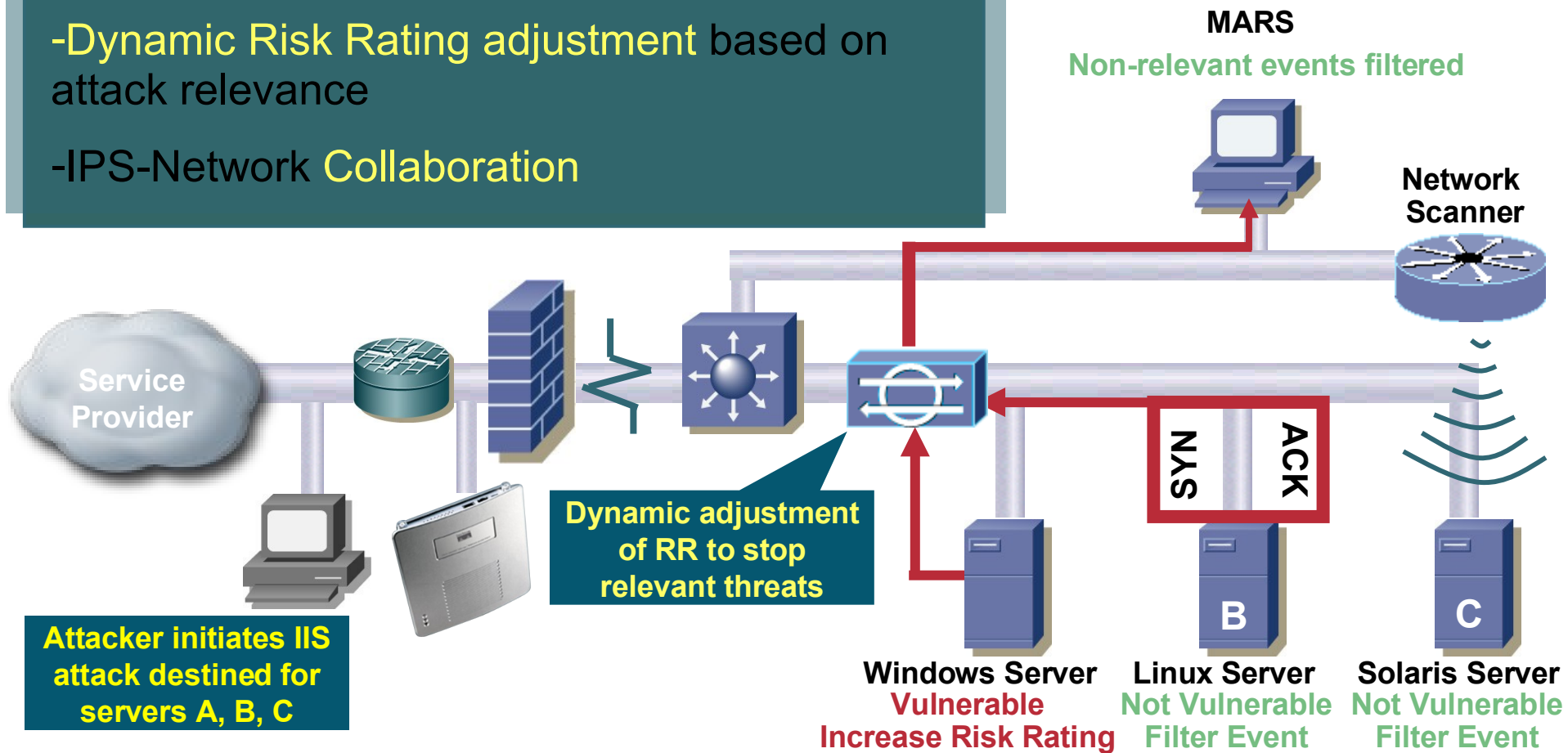
The screenshot shows the Cisco Systems WIDS configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', and 'COMMANDS'. The 'SECURITY' tab is active. The left sidebar shows 'Security' and 'AAA' options. The main content area is titled 'Signature > Detail' and shows configuration for a signature named 'NULL probe resp 1'. The configuration includes: Precedence: 2, Name: NULL probe resp 1, Description: NULL Probe Response - Zero length SSID element, Type: Management, Report: 1, Per Mac: 1, Mac Frequency: 1 (pkts/sec), and a checkbox that is checked. Below the configuration is a table with columns 'Pattern' and 'Mask'.

Pattern	Mask
0050	0x00ff
0000	0xffff

- Per-packet examination of WLAN protocols
- Seek specific pattern in WLAN data payload
- Note that it may also be useful to characterize the signature traffic—i.e., source, rate, time, etc.
- Database of known WIDS is maintained at controller

Cisco IPS

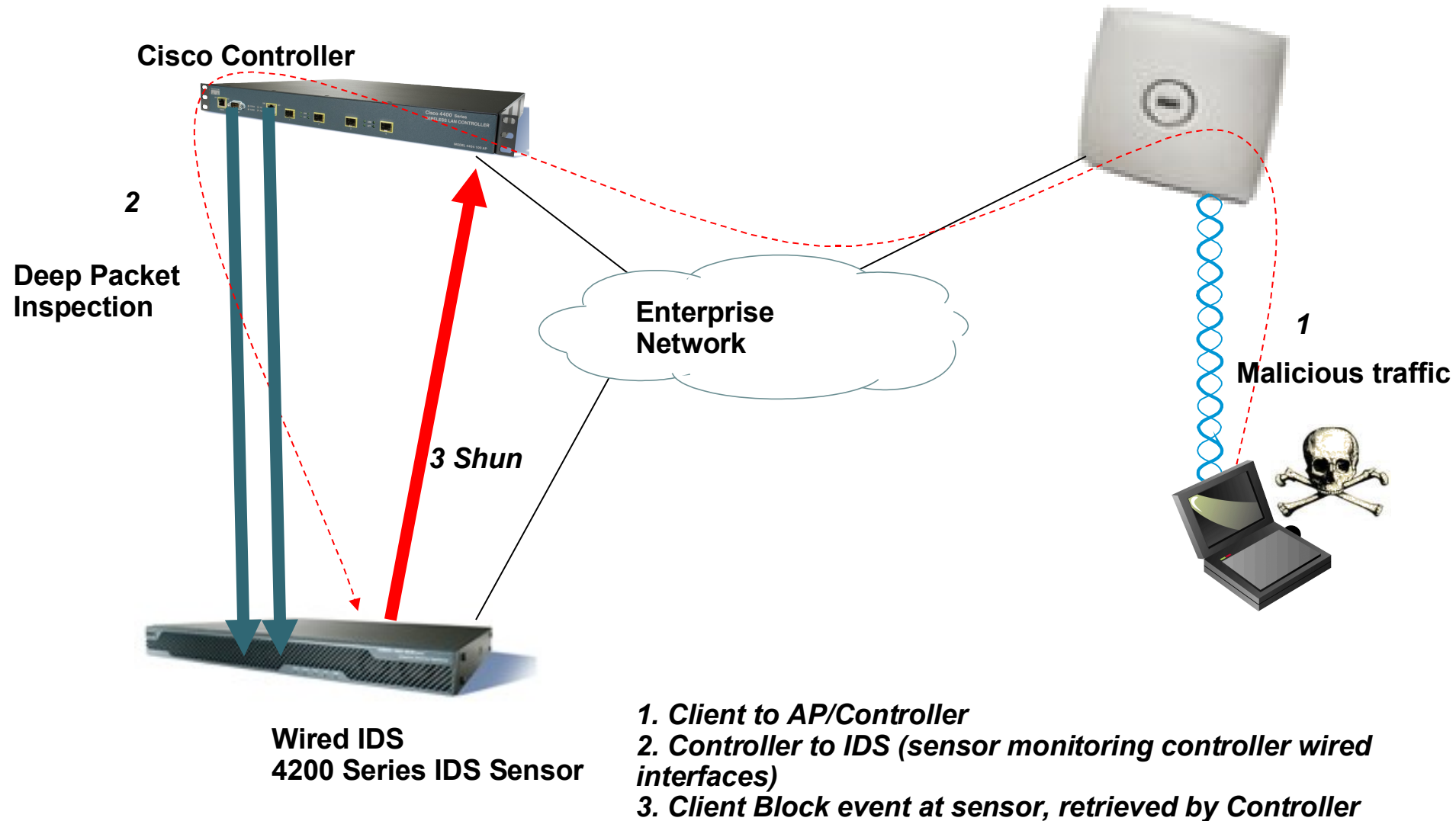
- Anomaly Detection / Network behavioral analysis
- Dynamic Risk Rating adjustment based on attack relevance
- IPS-Network Collaboration



Integración sensores Cisco IDS/IPS - Client Shunning



Evento IDS y Bloqueo del cliente



IDS Host Block/ Client Shun

The screenshot shows the Cisco IDM 5.0 - 10.0.1.4 interface. The left sidebar contains a tree view with 'Active Host Blocks' selected. The main area is titled 'Active Host Blocks' and contains the instruction 'Specify the address to block and the duration for that block.' Below this is a table with the following data:

Source IP	Destination IP	Destination Port	Protocol	Minutes Remaining	Timeout (minutes)	
10.0.1.28	10.0.1.22	31337	6	19		Add

Buttons for 'Add' and 'Delete' are located to the right of the table. A red circle highlights the 'Source IP' '10.0.1.28' in the table, with a red arrow pointing to the text 'Client Blocking/ Client Exclusion Event'.

Client Blocking/ Client Exclusion Event

The screenshot shows the Cisco Systems Security Management interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'SECURITY' tab is active. The left sidebar shows 'Security' with 'AAA' expanded. The main area is titled 'CIDS Shun List' and contains a 'Re-sync' button and a table with the following data:

IP Address	Last MAC Address	Expire	Sensor IP / Index
10.0.1.28	00:06:d7:86:38:42	29	10.0.1.4 / 1

A red circle highlights the 'IP Address' '10.0.1.28' in the table, with a red arrow pointing from the 'Active Host Blocks' table in the previous screenshot.



CISCO