Consiglio Nazionale delle Ricerche

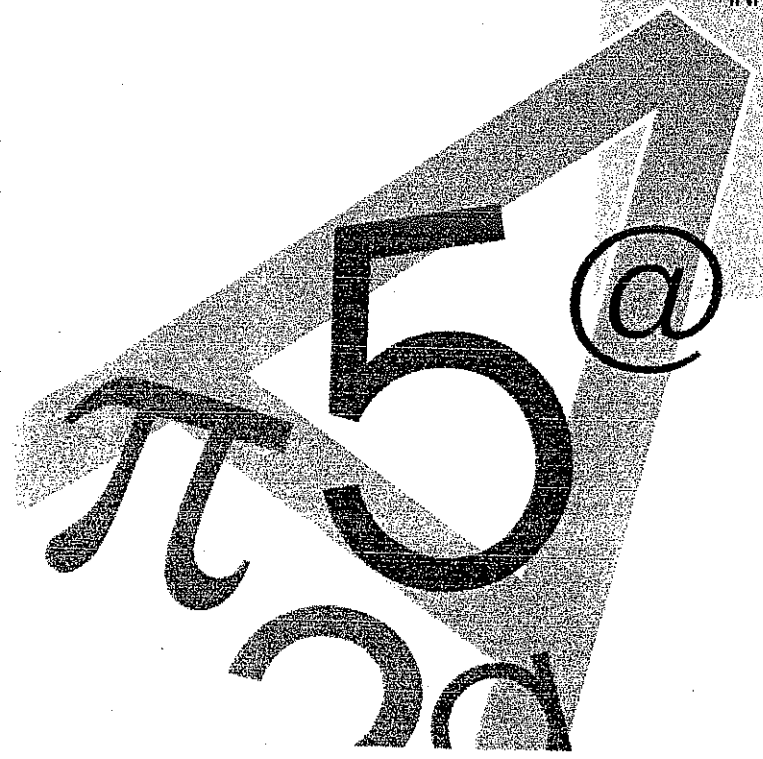
NOTA TECNICA

Organizzazione del Firewall della Direzione/Amministrazione dell'IEI

Carlo Carlesi

Luglio 2002
B4 07

I.E.I.
ISTITUTO DI
ELABORAZIONE DELLA
INFORMAZIONE



Organizzazione del Firewall della Direzione/Amministrazione dell'IEI

Carlo Carlesi

Luglio 2002

Introduzione

Scopo della presente nota e' quello di descrivere l'organizzazione della rete telematica di Direzione e Amministrazione dell'IEI, sottoposta per motivi di sicurezza, al controllo degli accessi via "firewall". Questa nota quindi si limita semplicemente a fare una fotografia della struttura della sottorete, riportando le informazioni strettamente necessarie al mantenimento ed aggiornamento della stessa. Nella sezione "Cablaggio Rete" descriviamo la struttura fisica indicando sia le stanze che i numeri delle prese controllate dal "firewall". Nella sezione "Regole di accesso" descriviamo brevemente le regole di accesso stabilite ed implementate con il software " FireWall-1".

1 Cablaggio Rete.

Dal punto di vista del cablaggio fisico, tutte le prese di rete nella zona della Direzione ed Amministrazione dell'IEI, sono attestate nell'armadio T11.1 riportato in figura 1.

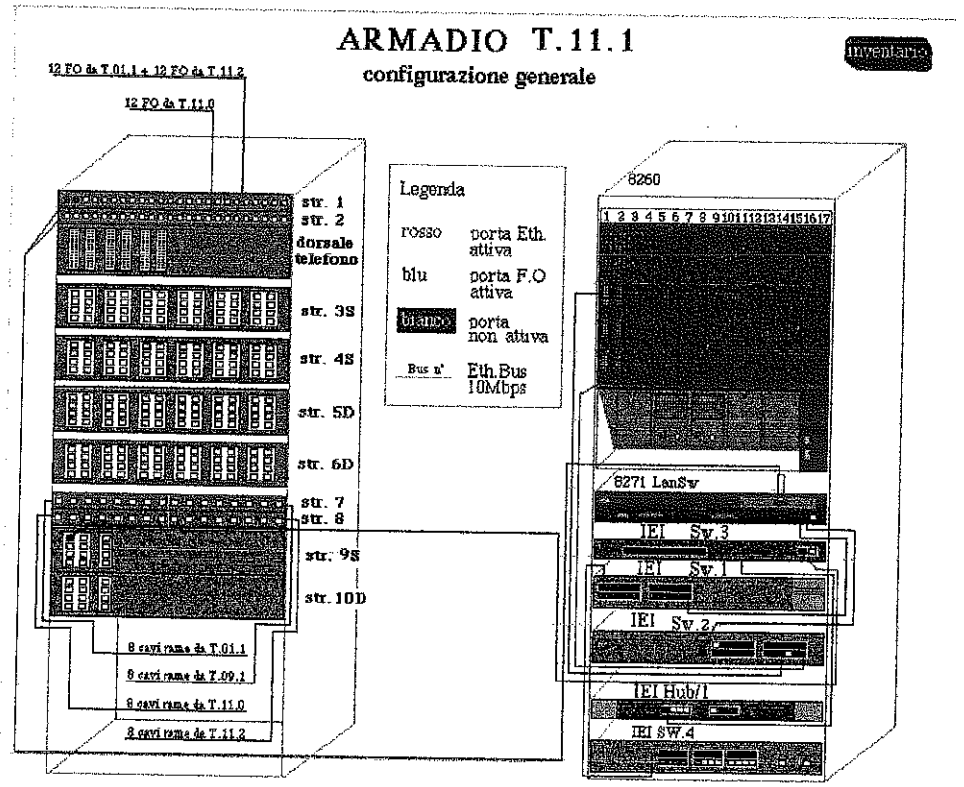


Figura 1

Per realizzare la sottorete fisica controllata dal firewall e' stato deciso di collegare le prese di interesse allo "Switch" indicato in figura 1 come "IEI Sw.3" e di seguito detto "Cisco".
Caratteristiche "Cisco".

Cisco "Catalist 1900" e' uno switch dotato di 12 porte a 10MB (numerate da 1-12) e di due porte a 100MB (indicate come A e B). Dovendo disporre di un numero di porte maggiore di 12 e' stato aggiunto in cascata allo switch Cisco, un "HUB" con ulteriori 8 porte a 10MB (indicato in figura 1 come "IEI HUB/1).

A questo punto possiamo notare che la porta 12 del Cisco serve da collegamento alla porta 1 dello HUB. La porta Cisco "A" che nella figura 1 si vede collegata ad una presa della parte sinistra dell'armadio, in realta' va direttamente su una porta a 100MB del sistema "Sun Ultra 1" che realizza il "Firewall" come descritto in figura 2.

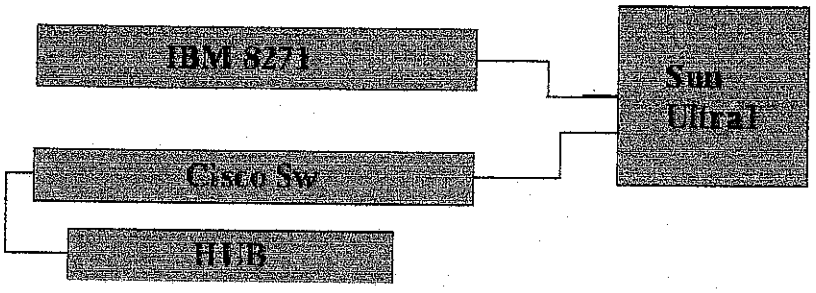


Figura 2

Caratteristiche "Sun Ultra 1".

"Sun Ultra 1", e' una sparcstation Sun Microsystem,con processore a 145MH e 196 MB di memoria centrale. Dispone di tre porte Ethernet di cui due a 100MB e una a 10MB. Il sistema operativo e' Solaris versione 5.1 ed il software utilizzato e' "Firewall-1" della Check Point.

Nella realizzazione del sistema "firewall" si sono utilzzate solo 2 interfacce Ethernet; con i seguenti indirizzi IP:

hme0:	192.168.85.1	(indirizzo privato);
le0:	194.119.192.254	(indirizzo pubblico).

La connessione alla rete di area avviene tramite un "Router-Cisco" con indirizzo IP:194.119.192.253 .

Il sistema software del firewall e' licenziato per supportare una classe c di indirizzi ed e' legato al "HostID" della macchina Sun Ultra 1.

Il sistema e' inoltre configurato per convertire in modalita' statica gli indirizzi privati (net. 196.168.85.xx) con gli indirizzi pubblici con cui le macchine sono registrate nel DNS del dominio IEI. Per convenzione si e' stabilito che le ultime 2 coppie di cifre

della rete privata "85.xx" corrispondano alle ultime due coppie di cifre della rete pubblica nel dominio iei.pi.cnr.it. Quindi la macchina con indirizzo privato 192.168.85.5 ad esempio corrisponde alla macchina 146.48.85.5 del dominio iei.
Le prese di rete che sono sottoposte al controllo del "firewall" sono quelle relative agli studi 1-5 e 9 (figura 3).

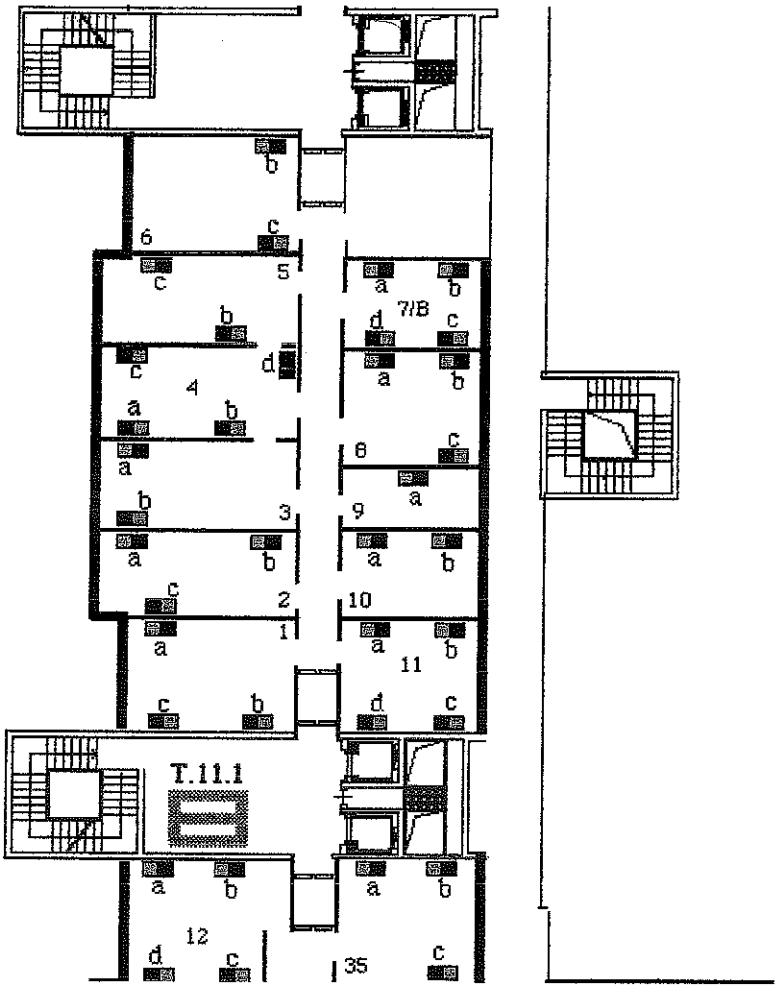


Figura 3

Mappa delle connessioni:

Codice presa	SW3	Codice presa	HUB/1
1b	SW3/1	SW3/12	1
1c	SW3/2		2
2c	SW3/3		3
2a	SW3/4		4
8a	SW3/5		5
	SW3/6		5
	SW3/7		6
4b	SW3/8	4d	7
4c	SW3/9	4d	8
5c	SW3/10		
9a	SW3/11		
HUB/1	SW3/12		

2 Regole di accesso.

Le regole di accesso stabilite sono estremamente semplici e si basano su le seguenti due norme:

A- Ogni macchina interna puo' aprire una qualsiasi connessione verso l'esterno;

B- Ogni accesso dall'esterno e' proibito se non esplicitamente consentito.

A seguito della norma B seguono alcune regole che abilitano solo alcune macchine esterne al firewall di collegarsi solo ad alcune macchine interne (amministrazione) e solo atrraverso specifici protocolli TCP/IP di comunicazione. La figura 4 riporta in versione grafica le 7 regole che implementano il controllo degli accessi alla rete di Direzione/Amministrazione dell IEI.

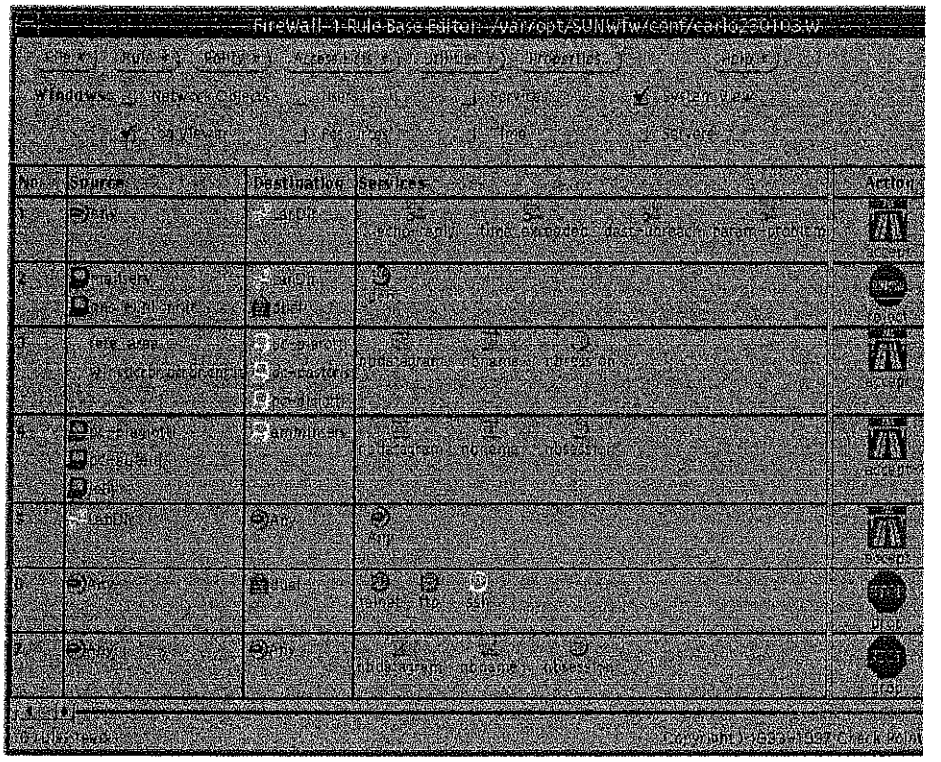


Figura 4

Per aggiungere o eliminare una macchina sia interna che esterna e' necessario intervenire solo da consolle del sistema Sun che ha un solo utente amministratore.