

# ACCESS CONTROL LIST (ACL)

# INTRODUZIONE ACL

LE ACL (ACCESS CONTROL LIST) SONO UNA LISTA DI ISTRUZIONI DA APPLICARE ALLE INTERFACCE DI UN ROUTER ALLO SCOPO DI GESTIRE IL TRAFFICO, FILTRANDO I PACCHETTI IN ENTRATA E IN USCITA.



# USO DEGLI ACL

ESISTONO SVARIATI MOTIVI PER CUI UTILIZZIAMO GLI ACL. IL MOTIVO PRINCIPALE È FORNIRE UN LIVELLO BASE DI SICUREZZA PER LA RETE. GLI ACL NON SONO COSÌ COMPLESSI E DI PROTEZIONE COME FIREWALL , MA FORNISCONO PROTEZIONE SU INTERFACCE AD ALTA VELOCITÀ IN CUI LA VELOCITÀ DELLA LINEA È IMPORTANTE, ED I FIREWALL POSSONO ESSERE RESTRITTIVI. GLI ACL VENGONO ANCHE UTILIZZATI PER LIMITARE GLI AGGIORNAMENTI PER IL ROUTING DAI PEER DI RETE, E POSSONO ESSERE DETERMINANTI NELLA DEFINIZIONE DEL CONTROLLO DI FLUSSO PER IL TRAFFICO DI RETE.

# DESCRIZIONE ACL

GLI ACL SONO UN FILTRO DI RETE UTILIZZATO DAI ROUTER E ALCUNI SWITCH, PER CONSENTIRE E LIMITARE I FLUSSI DI DATI IN ENTRATA E IN USCITA DALLE INTERFACCE DI RETE. QUANDO UN ACL È CONFIGURATO SU UN'INTERFACCIA, IL DISPOSITIVO DI RETE ANALIZZA I DATI CHE PASSANO ATTRAVERSO L'INTERFACCIA, LI CONFRONTA CON I CRITERI DESCRITTI NELL'ACL E CONSENTE AI DATI DI SCORRERE O VIETARLI.

ESISTONO DUE TIPI DI ACL:

- ACL STANDARD
- ACL ESTESE



# DIFFERENZE

LA DIFFERENZE TRA ACL STANDARD E ESTESE SONO:

- UN ACL STANDARD PUÒ CONSENTIRE O NEGARE IL TRAFFICO BASATO SOLO SUGLI INDIRIZZI DI ORIGINE.
- UN ACL ESTESO PUÒ CONSENTIRE O NEGARE IL TRAFFICO IN BASE AGLI INDIRIZZI DI ORIGINE E DI DESTINAZIONE, NONCHÉ AI TIPI DI TRAFFICO TCP (AFFIDABILTÁ COMUNICAZIONE TRA MITTENTE E DESTINATARIO) / UDP (PIÚ VELOCE MA NENO AFFIDABILE / ICMP (AVVERTE SE CI SONO MALFUNZIONAMENTI NELLA TRASMISSIONE)).

# TIPI DI ACL NEL DETTAGLIO

## Protocollo

## Range

### IP

Indica il Numero ed il nome delle ACL.

1-99

### Extended IP

Indica il numero e il nome delle ACL IP Estese.

100-199

### AppleTalk

AppleTalk era un protocollo molto usato nelle reti Macintosh. Il suo principale scopo era quello di condividere stampanti e/o file, e quindi metterli a disposizione degli utenti che facevano parte della rete.

600-699

### IPX

Protocollo variante delle IP usate nello scambio di pacchetti nelle reti network.

800-899

### Extended IPX

Protocollo variante delle Extended IP usate nello scambio di pacchetti nelle reti network.

900-999

### IPX Service Advertising Protocol

Aggiunge o rimuove servizi in una intranet IPX.

1000-1099



# DIFFERENZA TRA ACL E FIREWALL

GLI ACL ESEGUONO ISPEZIONI SENZA STATO, IL CHE SIGNIFICA CHE L'ELENCO DI ACCESSO ESAMINA UN PACCHETTO E NON HA ALCUNA CONOSCENZA DI CIÒ CHE È VENUTO PRIMA. SE UN ACL ESAMINA UN PACCHETTO CHE UTILIZZA TCP CON IL SET DI BIT ACK, L'ACL PUÒ SOLO CAPIRE CHE SI TRATTA DI UN PACCHETTO DI RICONOSCIMENTO. TUTTAVIA, NON È A CONOSCENZA SE ESISTE REALMENTE UNA CONVERSAZIONE A CUI APPARTIENE QUESTO PACCHETTO.

UN FIREWALL HA UN USO E UNO SCOPO PRINCIPALI ED È QUELLO DI ESAMINARE IL TRAFFICO CHE PASSA ATTRAVERSO UNA PARTE DELLA RETE E PRENDERE DECISIONI SU COSA LASCIARE E COSA BLOCCARE. DI SOLITO UN FIREWALL ESEGUE UN'ISPEZIONE DI STATO, IL CHE SIGNIFICA CHE IL FIREWALL NON VEDE SOLO IL PACCHETTO TCP CON IL BIT ACK IMPOSTATO, MA IL FIREWALL È IN GRADO DI SAPERE SE C'È STATO UN INIZIO CORRETTO PER QUESTA CONVERSAZIONE TCP.

# ESEMPIO DI COME APPLICARLE LE ACL

## Standard

## Extended

```
Router8
Physical Config CLI Attributes

(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team
Image text-base: 0x400A925C, data-base: 0x4372CE20

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wml/export/crypto/cool/stgrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
cisco 3811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID JAD06190MTZ (4292891495)
M860 processor: part number 0, mask 49
4 Ethernet/IEEE 802.3 interface(s)
2 FastEthernet/IEEE 802.3 interface(s)
239K bytes of non-volatile configuration memory.
62720K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team

Press RETURN to get started!

Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 1 deny 156.166.1.0 0.0.0.255
Router(config)#interface FastEthernet0/0
Router(config-if)#ip access-group 1 in
Router(config-if)#
```

```
Router8
Physical Config CLI Attributes

(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team
Image text-base: 0x400A925C, data-base: 0x4372CE20

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wml/export/crypto/cool/stgrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
cisco 3811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID JAD06190MTZ (4292891495)
M860 processor: part number 0, mask 49
4 Ethernet/IEEE 802.3 interface(s)
2 FastEthernet/IEEE 802.3 interface(s)
239K bytes of non-volatile configuration memory.
62720K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team

Press RETURN to get started!

$LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2/0, changed state to up

$LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

$LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 100 deny tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 80
Router(config)#access-list 100 deny tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 443
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#ip access-group 100 out
Router(config-if)#
```