
Firewall, NGFW & Co
Esperienze INFN
tips & tricks

“*As security or firewall administrators, we’ve got basically the same concerns as plumbers: the size of the pipe, the contents of the pipe, making sure the correct traffic is in the correct pipes, and keeping the pipes from splitting and leaking all over the place. Of course, like plumbers, when the pipes do leak, we’re the ones responsible for cleaning up the mess, and we’re the ones who come up smelling awful.*”

—*Marcus J. Ranum, esperto in implementazione di sistemi di sicurezza*

“*If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.*”

—*Bruce Schneier, crittografo*

INTRODUZIONE

Di cosa parliamo

Network Security

Definizioni e individuazione del perimetro

Quali tipologie di attacco

Qualche dato

Come interveniamo

Regole e comportamenti

Dispositivi di protezione

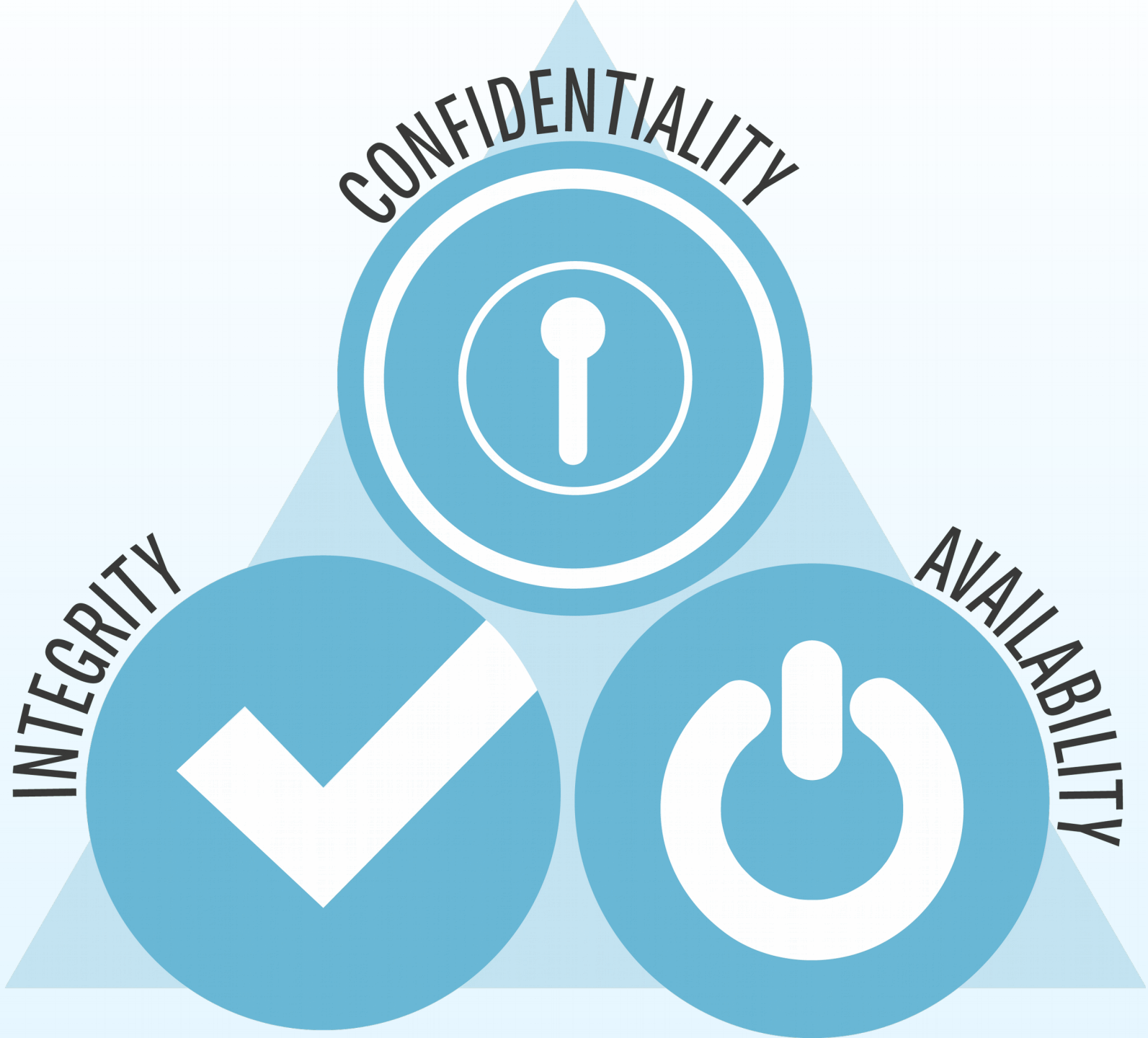
Gestione e controllo degli eventi

…e la comunità accademica e della ricerca ?

Siamo diversi ?

Abbiamo peculiarità ?

Quali dati, quali strutture ?


CONFIDENTIALITY
INTEGRITY
AVAILABILITY

CIA Triad

CIA: non è un'agenzia straniera di Intelligence ma si riferisce ai princìpi minacciati dal cybercrime che devono essere difesi

The inter-relationship between confidentiality, integrity, and availability is critical to establishing policies and procedures in information technology security

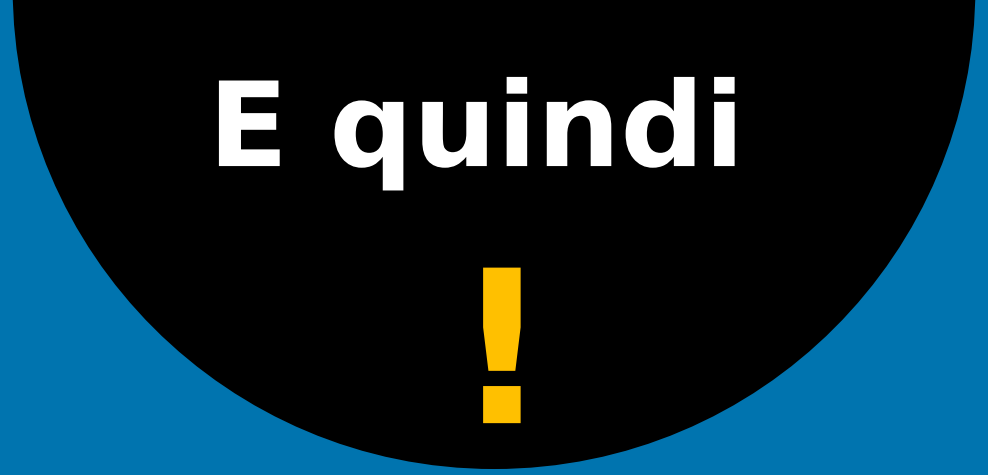
"Confidenzialità"	"Integrità"	"Disponibilità"
Solo i soggetti autorizzati possono avere accesso ad una risorsa	**Una risorsa può essere modificata solo dai soggetti e nei modi autorizzati**	**Una risorsa è accessibile ai soggetti autorizzati al momento appropriato**
permessi dei file	hashing	HA clusters
access control lists	version control system	failover redundancy systems
cifratura	backup	disaster recovery capabilities

VIDEO dal campo di battaglia

VIDEO - NSE 1 Fortinet Bad Actors

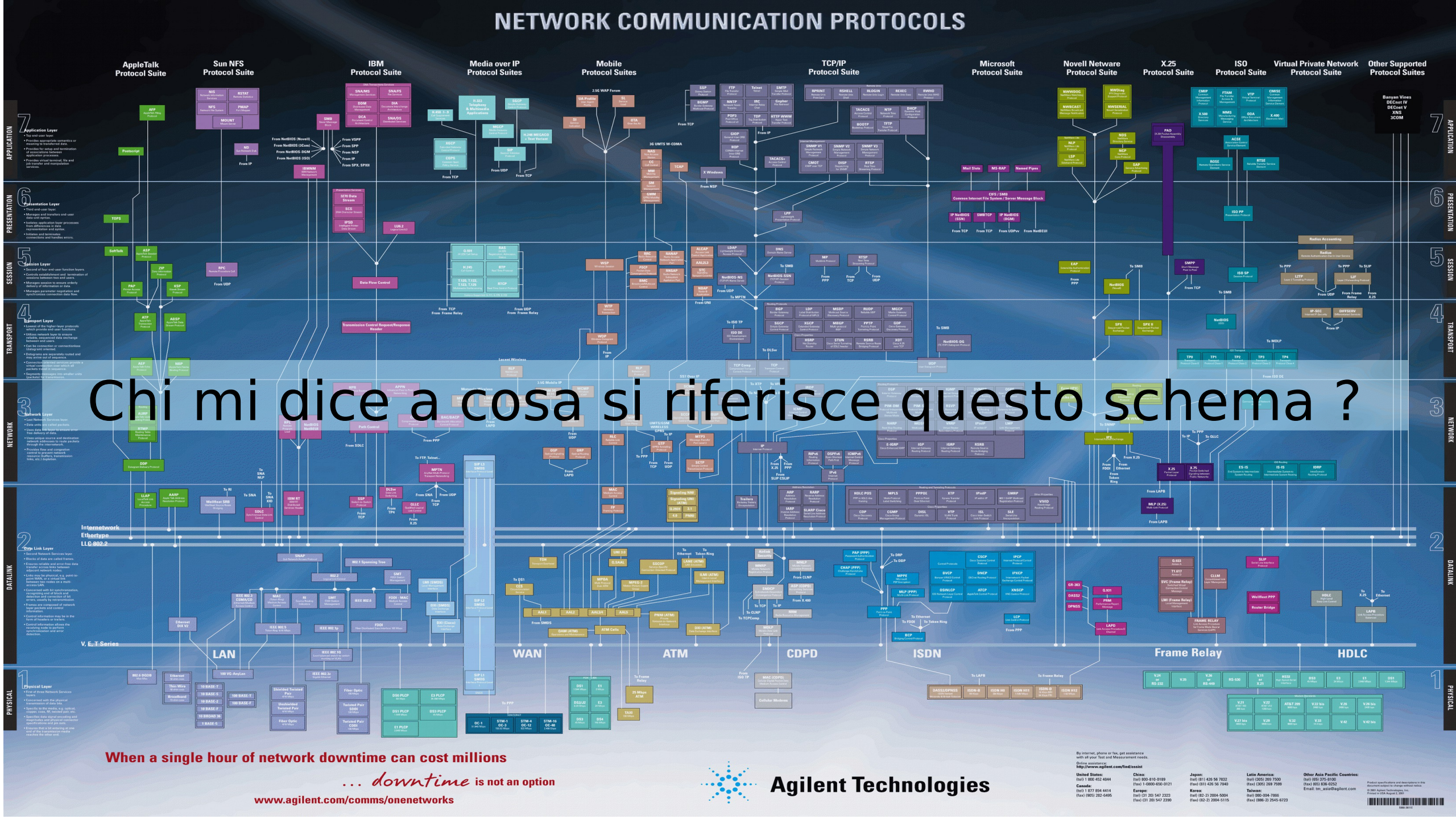
Richiede registrazione e autenticazione

https://training.fortinet.com/course/index.php?categoryid=3



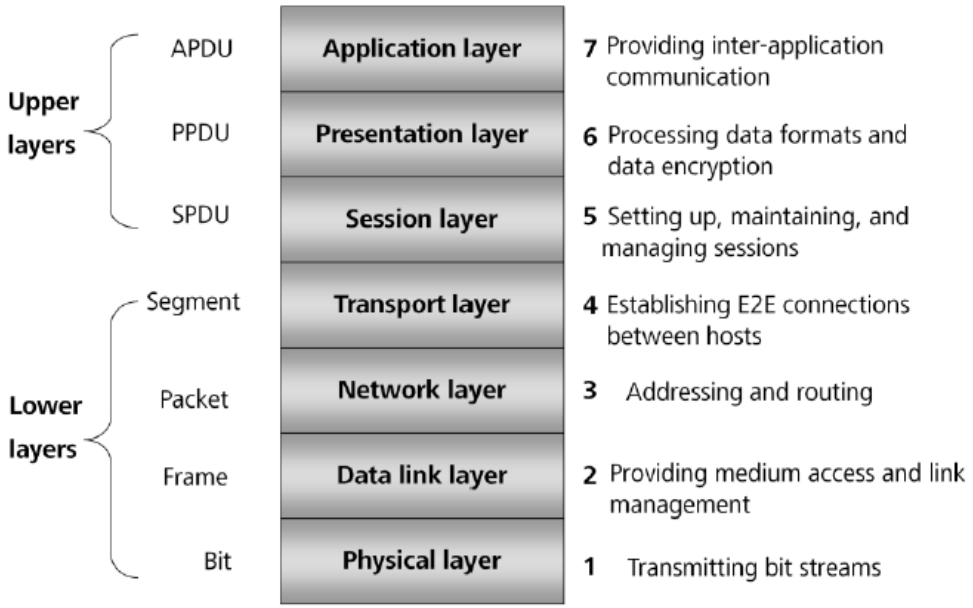
....torniamo a noi

Portiamo l’attenzione sulla rete... e partiamo dall’inizio


NETWORK COMMUNICATION PROTOCOLS
AppleTalk Protocol Suite
Sun NFS Protocol Suite
IBM Protocol Suite
Media over IP Protocol Suites
Mobile Protocol Suites
TCP/IP Protocol Suite
Microsoft Protocol Suite
Novell Netware Protocol Suite
X.25 Protocol Suite
ISO Protocol Suite
Virtual Private Network Protocol Suite
Other Supported Protocol Suites
Banyan Vines
DECnet IV
DECnet V
XNS
3COM
APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
DATALINK
PHYSICAL
Chi mi dice a cosa si riferisce questo schema ?
Internetwork
Ethertype
LLC 802.2
LAN
WAN
ATM
CDPD
ISDN
Frame Relay
HDLC
When a single hour of network downtime can cost millions
. . . downtime is not an option
www.agilent.com/comms/onenetworks
Agilent Technologies

Encapsulation means that a network node packetizes the data to be transmitted with a specific **protocol header** and also refers to adding a packet to the end of the data at some layers for processing. Each layer in the OSI model encapsulates data to ensure that the data properly reaches the destination and is received and executed by the terminal host

Introduction to the Seven Layers of the OSI Model

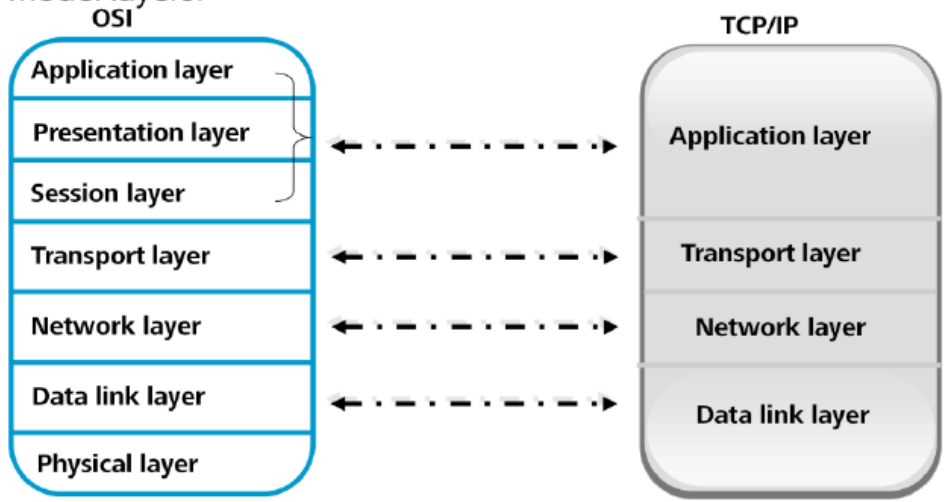


Copyright © 2015 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Mapping Between the TCP/IP Model and OSI Model

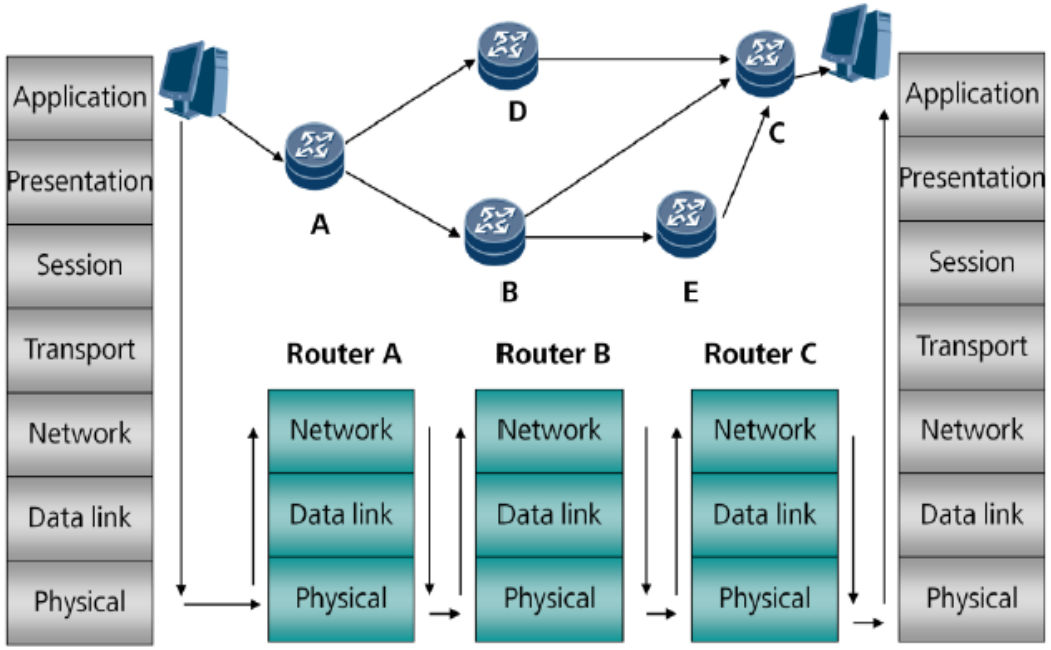
- TCP/IP is simply tiered, and its layers clearly map with OSI model layers.



Copyright © 2015 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Procedure for Processing Network Data Streams



Copyright © 2015 Huawei Technologies Co., Ltd. All rights reserved.

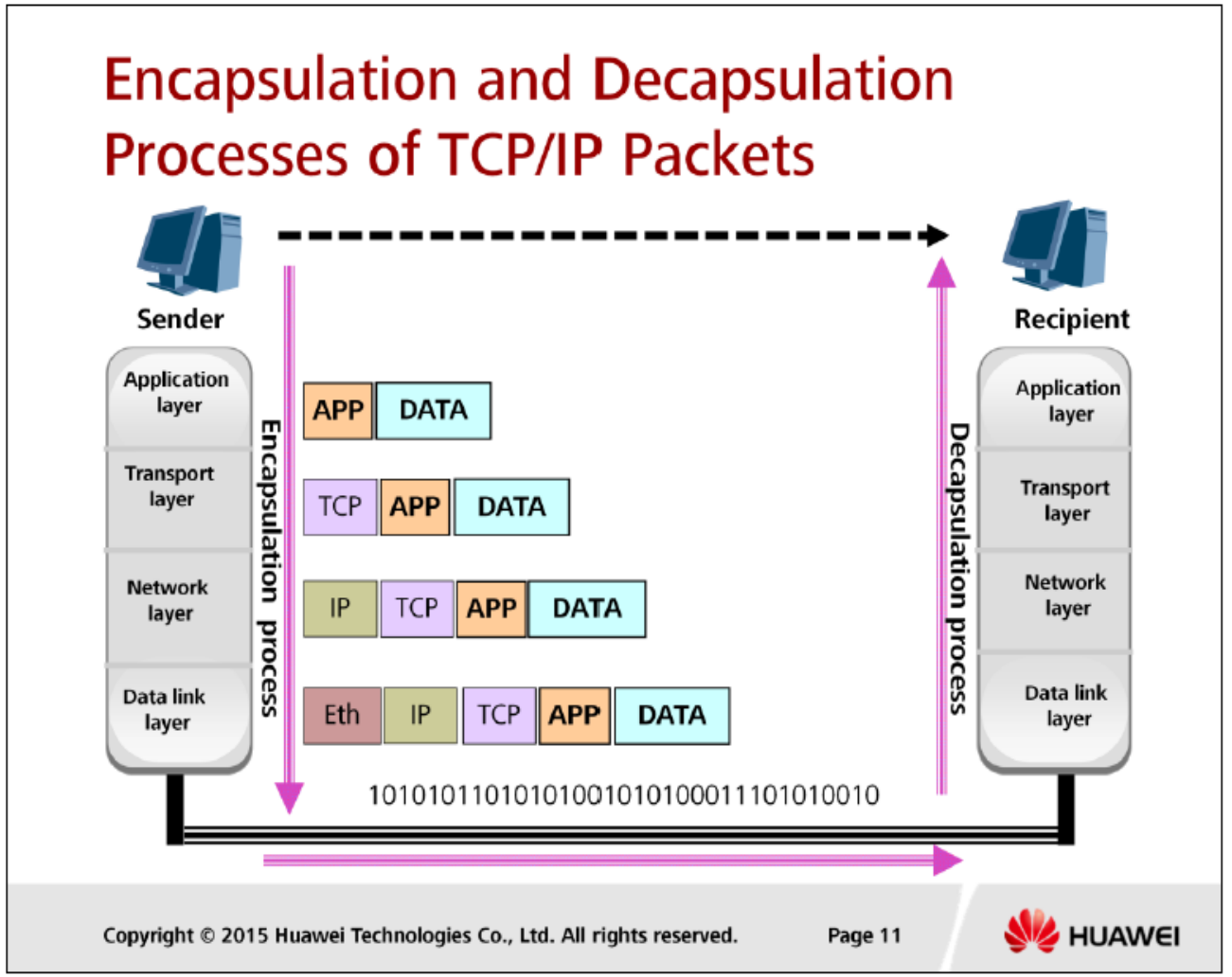
HUAWEI

Procedure for processing network data streams:

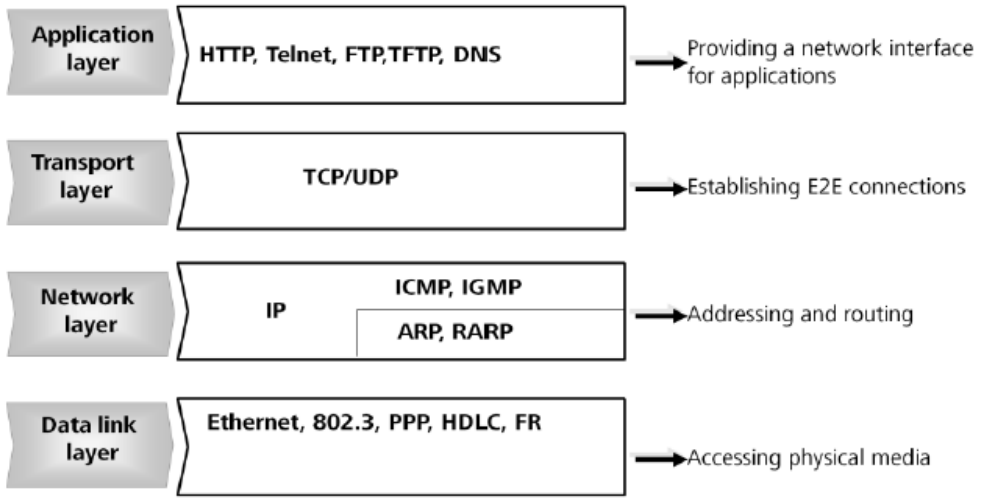
1. When an application on a network host needs to send a packet to a destination on another network, one interface of the router **on the same network** of the host receives the **frame**
2. The **data link layer** of the router checks the frame, determines the carried data type at the network layer, **removes the frame head**, and sends the data to the corresponding network layer
3. The **network layer** checks the packet header to determine the network segment of the destination and obtains the **next-hop** interface by looking up the **routing table**
4. The **data link layer of the next-hop** interface **adds a frame header** to the **packet,** encapsulates the packet as a frame, and sends it to the next hop. Forwarding of each packet follows this process
5. **After reaching the network of the destination host**, the packet is **encapsulated** as the frame at the data link layer of the destination network and sent to the target host
6. After the destination host receives the packet, **the frame**

Data encapsulation process is as follows:

1. Data is sent to the **application layer** first and added with application-layer information
2. After being processed by the application layer, the **packet** is sent to the **transport layer** and added with transport-layer information, for example TCP or UDP
3. After being processed by the transport layer, the packet is sent to the **network layer** and added with network-layer information (such as IP protocol)
4. After being processed by the network layer, the packet is sent to the **data link layer** and added with data link-layer information (such as Ethernet, 802.3, PPP, and HDLC).
5. Then, data is transmitted to the peer-end in **bit stream** format. (In this process, processing methods vary with device types. In general, switches process data link-layer information, whereas routers process network-layer information. The data is restored only when it reaches the



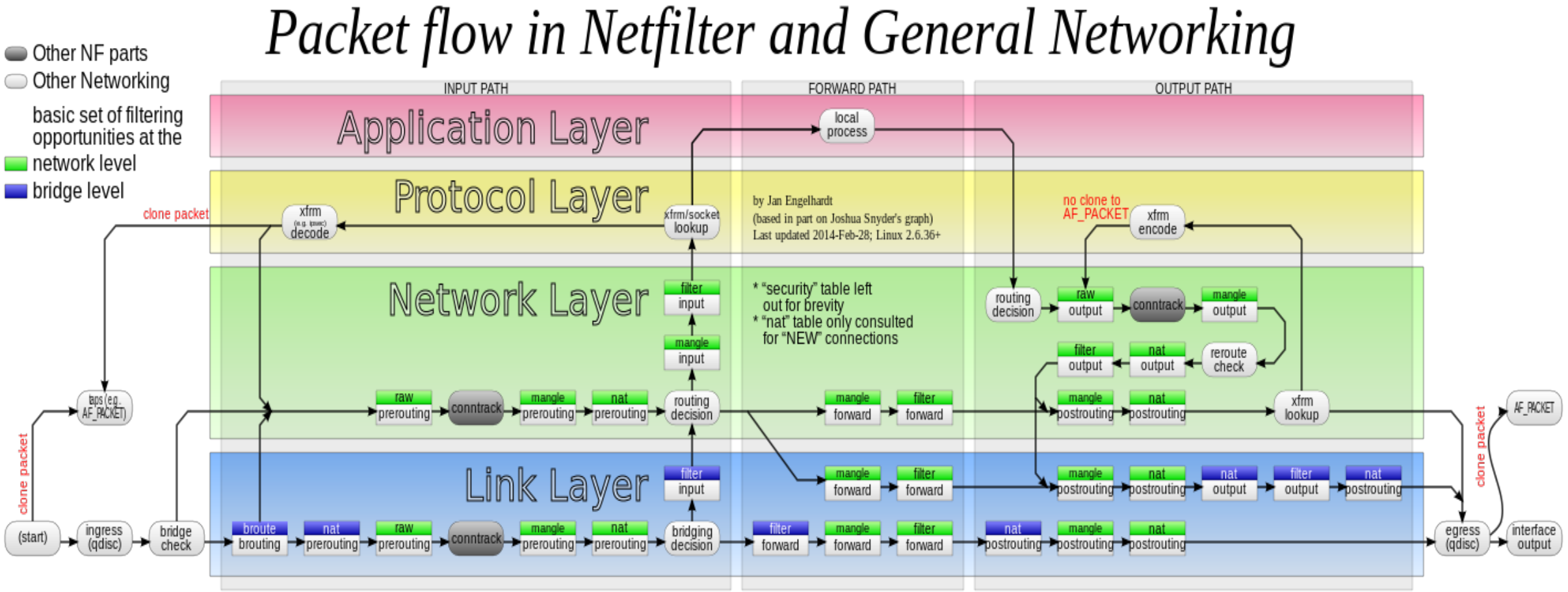
Functions of Each TCP/IP Layer

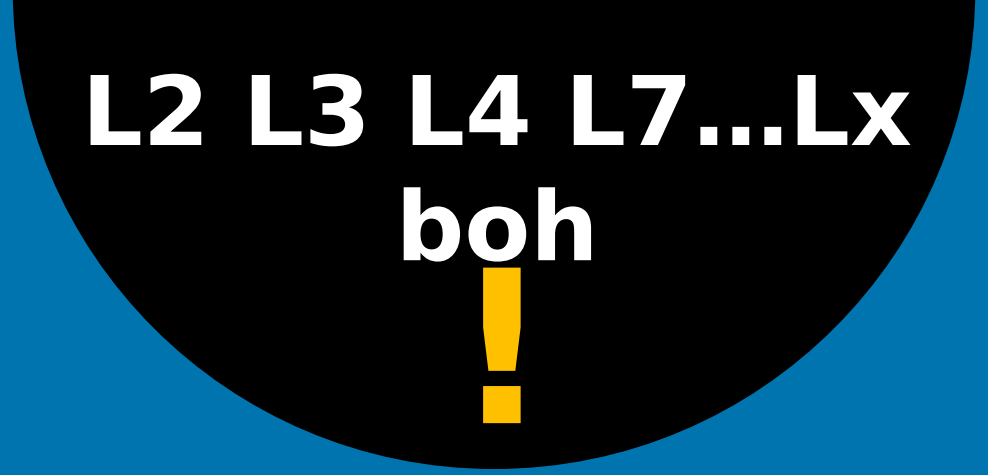


Copyright © 2015 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Linux


Packet flow in Netfilter and General Networking
Other NF parts
Other Networking
basic set of filtering opportunities at the network level
bridge level
INPUT PATH
FORWARD PATH
OUTPUT PATH
Application Layer
Protocol Layer
Network Layer
Link Layer
local process
clone packet
xfrm (e.g. ipsec) decode
xfrm/socket lookup
by Jan Engelhardt
(based in part on Joshua Snyder's graph)
Last updated 2014-Feb-28; Linux 2.6.36+
no clone to AF_PACKET
xfrm encode
filter input
mangle input
* "security" table left out for brevity
* "nat" table only consulted for "NEW" connections
routing decision
raw output
conntrack
mangle output
filter output
nat output
reroute check
taps (e.g. AF_PACKET)
raw prerouting
conntrack
mangle prerouting
nat prerouting
routing decision
mangle forward
filter forward
mangle postrouting
nat postrouting
xfrm lookup
clone packet
AF_PACKET
filter input
mangle forward
filter forward
mangle postrouting
nat postrouting
nat output
filter output
nat postrouting
(start)
ingress (qdisc)
bridge check
broute brouting
nat prerouting
raw prerouting
conntrack
mangle prerouting
nat prerouting
bridging decision
filter forward
mangle forward
filter forward
nat postrouting
mangle postrouting
nat postrouting
egress (qdisc)
interface output



A quale livello operano i Firewall?

Esistono differenti tipologie di firewall che agiscono a livelli differenti?

“

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.[1] A firewall typically establishes a barrier between a trusted internal network and untrusted outside network, such as the Internet.[2]

https://en.wikipedia.org/wiki/Firewall_(computing)

FIREWALL RULES

https://it.wikipedia.org/wiki/Firewall

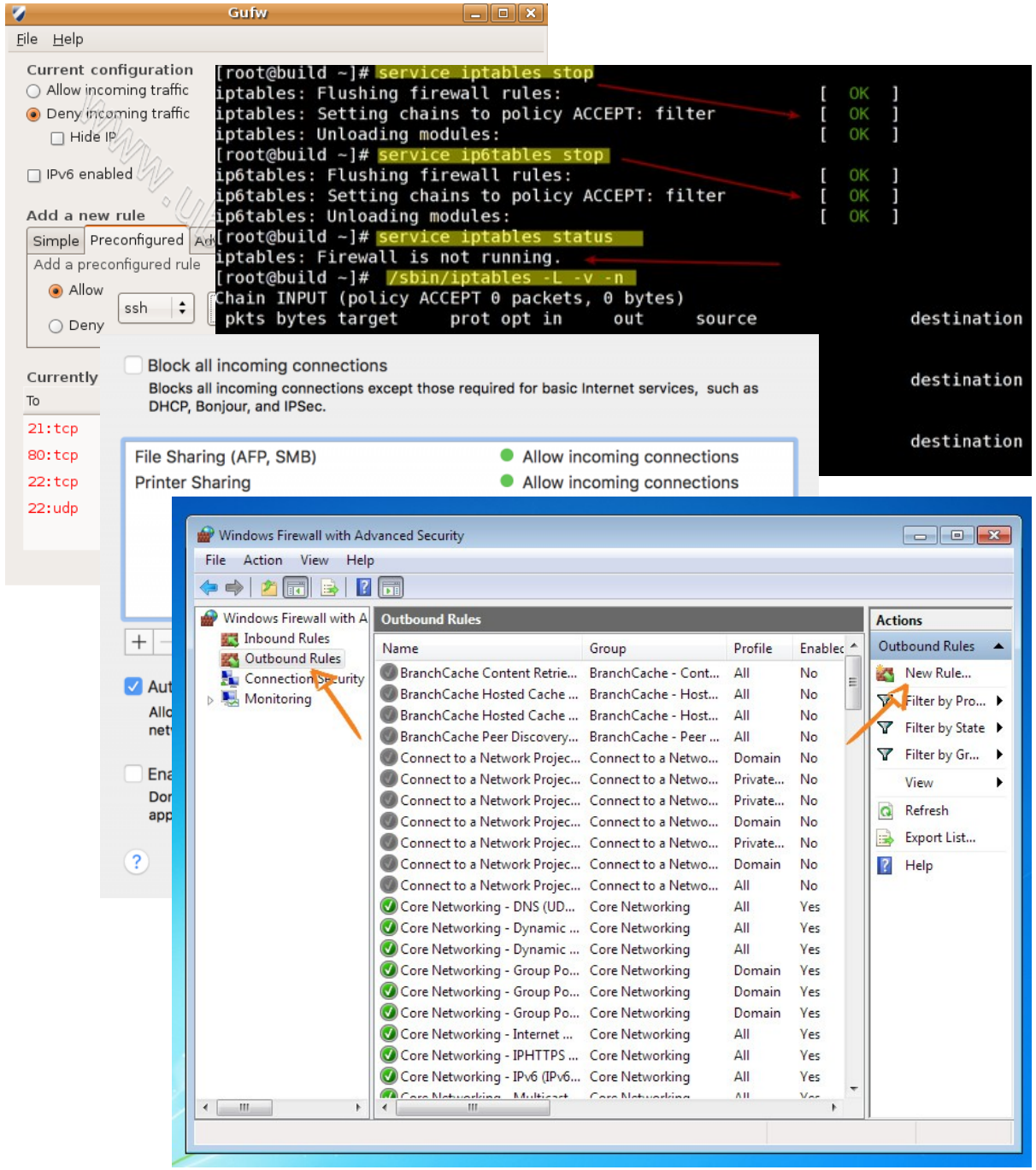
Un firewall filtra il traffico sulla base di un insieme di regole che lo fanno conformare con una policy di sicurezza.[1][2][4][7][9][10][13] Esistono due politiche per l'applicazione delle regole:

- policy default-deny: viene permesso solo ciò che viene dichiarato esplicitamente, il resto viene vietato;
- policy default-allow: viene vietato solo ciò che viene dichiarato esplicitamente, il resto viene permesso.[1][15]

L'analisi dei pacchetti che costituiscono il traffico, secondo i criteri di sicurezza formalizzati dalle regole, si traduce in una delle seguenti azioni:

- allow: il firewall lascia passare il pacchetto;
- deny: il firewall blocca il pacchetto e lo rimanda al mittente;
- drop: il firewall blocca il pacchetto e lo scarta senza inviare alcuna segnalazione al mittente.[1][13]

Di solito i firewall non prevedono il blocco del pacchetto e il rinvio dello stesso al mittente per evitare uno spreco di banda.[13]

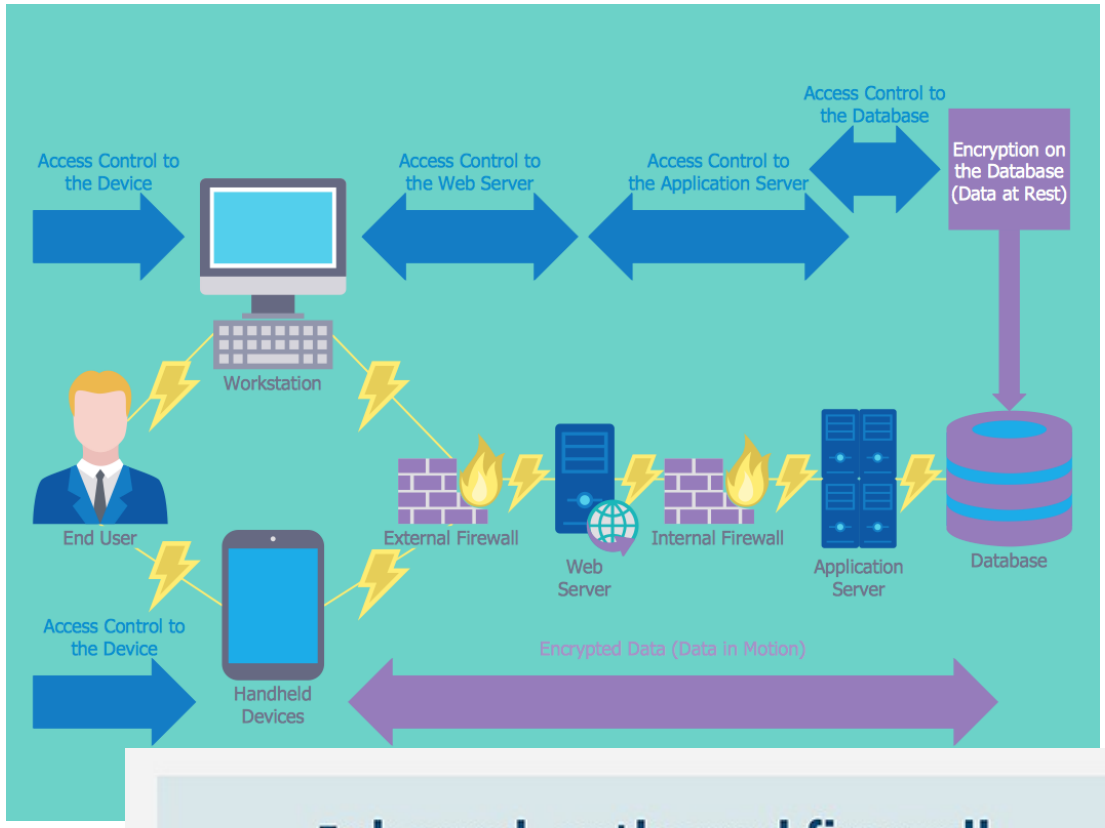


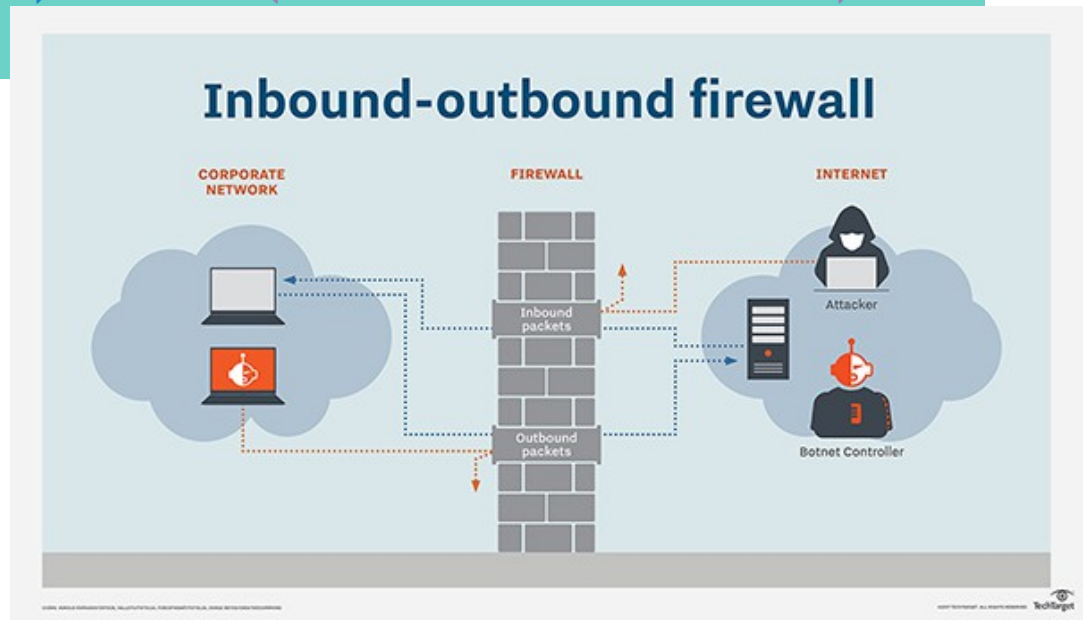
Host-based o Personal Firewall

Protegge i sistemi utente

- controlla il traffico entrante e uscente da un computer
- è in grado di prendere decisioni analizzando tutti i livelli OSI

Network-based Firewall





E’ un componente hardware stand-alone che viene posto sul confine di una rete in modo da filtrare tutto il traffico che questa scambia con l'esterno

Per questo viene anche detto *firewall perimetrale*[14]

Dato che vengono impiegati per separare una rete interna da una rete esterna, sono dotati di almeno due interfacce di rete

Firewall evolution

Le generazioni tecnologiche dei firewall si sono evolute dai primi anni 70 ad oggi, creando almeno tre tipologie genotipiche nessuna delle quali ancora estinta

First: Packet filter o stateless firewall da tutti conosciuti come ACL.

Filtrano il traffico basandosi su 5 informazioni dell' intestazione del pacchetto di L3

sorgente:porta:destinazione:porta:protocollo

Secondo: **Stateful** firewall

Filtrano il traffico considerando anche il L4 della pila OSI

Mantengono in memoria una tabella delle sessioni permettendo così la stateful inspection completa. Prendono la decisione al completamento di una fase riconosciuta della trasmissione

Third: Application Layer firewall

Filtrano il traffico considerando tutto lo stack OSI

Sono in grado di prendere decisioni analizzando l'intero contenuto informativo

NGFirewall +Funzioni

L’ultima generazione integra tutte le caratteristiche delle precedenti alla deep packet inspection consentendo anche funzioni aggiuntive

First: IDS/IPS

Gli **IDS** sono meccanismi di *analisi del traffico* di rete (**NIDS**) o di *funzionamento* dei sistemi (**HIDS**) che basandosi su confronti signature based o anomaly based rilevano violazioni di policy prestabilite, generando un allarme.

Nel caso pongano in atto azioni correttive vendono chiamati **IPS**

Second: Identity management integration

Sono le funzioni che permettono *di abilitare* un utente o un dispositivo a specifiche funzionalità di rete stabilite da policy, solo *in seguito ad autenticazione ed autorizzazione*.

Third: WAF

Il Web Application Firewall è un tipo particolare di Firewall che *prende decisioni analizzando il contenuto informativo di una sessione http*. E’ in grado in questo modo di filtrare malware tipico delle web app

Firewall non Firewall

Esistono altre due categorie di funzionalità di rete che pur non essendo propriamente firewall hanno assunto un ruolo non secondario nella protezione della rete

First: Proxy Firewall

Un proxy server può comportarsi come un app Firewall e decidere quali richieste utente propagare e quali risposte inoltrare basandosi su regole. Risulta così in grado di isolare le due reti coinvolte

Second: NAT & Co.

Sebbene I meccanismi di traduzione di indirizzo non siano nati da esigenze di protezione , realizzano a tutti gli effetti una rete “naturalemente” isolata INBOUND e quasi trasparente OUTBOUND

Consente anche l’ottimizzazione degli spazi di indirizzo

NGFirewall cont’

I dispositivi di ultima generazione aggiungono alle caratteristiche di Firewall funzioni aggiuntive non propriamente di filtro dei pacchetti

First: VPN

Circuito di rete virtuale tipicamente punto punto realizzato attraverso un tunnel cifrato incapsulato all’interno del protocollo IP o a livello applicativo.

Consente il passaggio sicuro dei dati attraverso la rete geografica o comunque una rete insicura

Second: Captive Portal Portale HTTP nel quale si autorizza un utente che fornisce le proprie credenziali all’acceso ad una rete altrimenti protetta

Third: SSL decryption Capacità di decifrare realtime le sessioni SSL (HTTPS) per analizzarne il contenuto.

https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Implement-and-Test-SSL-Decryption/ta-p/59719



Ora possiamo definire un NGFW

E la definizione non la prendiamo da wikipedia ma da Gartner

NGFW (Gartner def.)

are *deep-packet inspection* firewalls that move beyond port/protocol inspection and blocking to add *application-level* inspection, *intrusion prevention*, and bringing intelligence from outside the firewall. An NGFW should not be confused with a stand-alone network intrusion prevention system (IPS), which includes a commodity or nonenterprise firewall, or a firewall and IPS in the same appliance that are not closely integrated

https://www.gartner.com/it-glossary/next-generation-firewalls-ngfws

Sono Firewall di terza generazione che realizzano filtri applicativi basati su signature

Sono sistemi di Intrusion Prevention System basati su **signature**

Possono realizzare ***threat control* real-time** basato su signature come AntiVirus, AntiMalware e Anti Spam

Firewall e IPS sono integrati rendendo possibile realizzare **policy complesse**

Possibilità di **incorporare informazioni** che provengono **dall'esterno** quali policy basate su LDAP, whitelist e blacklist,etc

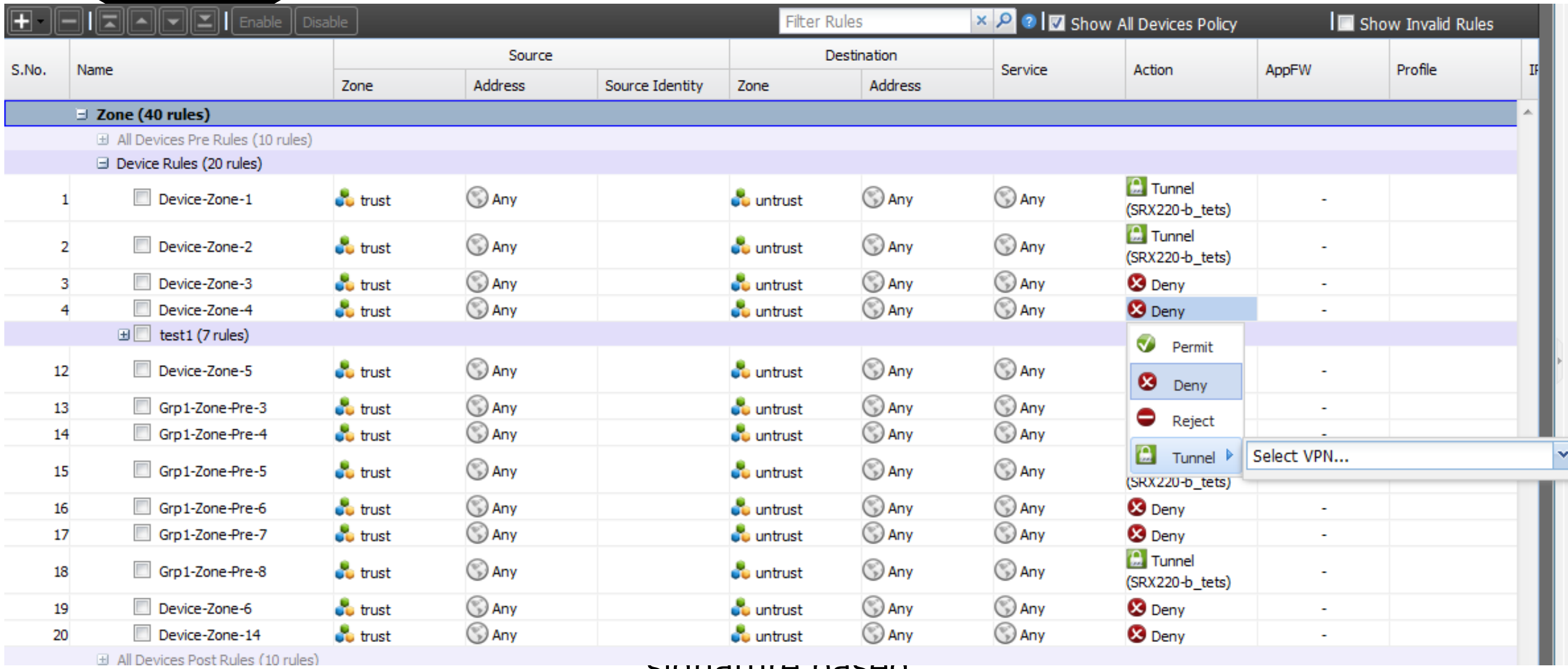
http://www.mydigitalshield.com/traditional-firewalls-vs-next-generation-firewalls/

https://

```
R1(config-ext-nacl)#do sh access-list OutBoundAccess
Extended IP access list OutBoundAccess
    10 permit ip 192.168.1.0 0.0.0.255 any
    11 deny tcp 192.168.2.0 0.0.0.127 any eq smtp
    12 deny tcp 192.168.2.0 0.0.0.127 any eq sunrpc
    13 deny tcp 192.168.2.0 0.0.0.127 any eq pop2
    14 deny tcp 192.168.2.0 0.0.0.127 any eq nntp
    15 deny tcp 192.168.2.0 0.0.0.127 any eq ftp
    16 deny tcp 192.168.2.0 0.0.0.127 any eq ftp-data
    17 deny tcp 192.168.2.0 0.0.0.127 any eq telnet
    18 deny tcp 192.168.2.0 0.0.0.127 any eq cmd
    19 deny tcp 192.168.2.0 0.0.0.127 any eq irc
    20 permit ip 192.168.2.0 0.0.0.255 any
    30 permit ip 192.168.3.0 0.0.0.255 any
    40 permit ip 192.168.4.0 0.0.0.255 any
    50 permit ip 192.168.5.0 0.0.0.255 any
R1(config-ext-nacl)#
```

ESEMPI

Facciamo alcuni esempi di policy. ACL Stateful e NGFW



signature based

Vengono introdotti controlli a livello di user e host

ESEMPI

Facciamo alcuni esempi di policy. ACL Stateful e NGFW

- Security
- NAT
- QoS
- Policy Based Forwarding
- Decryption
- Application Override
- Captive Portal
- DoS Protection

Addresses

Name	Address

		Source				Destination				
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
TRUST-TRUST	none	Trust	any	any	any	Trust	any	any	any	✓
DMZ-DMZ	none	DMZ	any	any	any	DMZ	any	any	any	✓
DMZ-TRUST	none	DMZ Trust	any	any	any	DMZ Trust	any	any	any	✓
DMZ-Untrust	none	DMZ	any	any	any	Untrust1	any	any	any	✓
Trust-Untrust1	none	Trust	any	any	any	Untrust1	any	any	any	✓
Untrust1-Trust	none	Untrust1	any	any	any	Untrust1	any	ike ipsec panos-global-... panos-web-in... ssl	any	✓
DENY ALL	none	any	any	any	any	any	any	any	any	⊘

signature based

Vengono introdotti controlli a livello di user e host

ADESSO PASSIAMO AD ALCUNE USER GUIDE

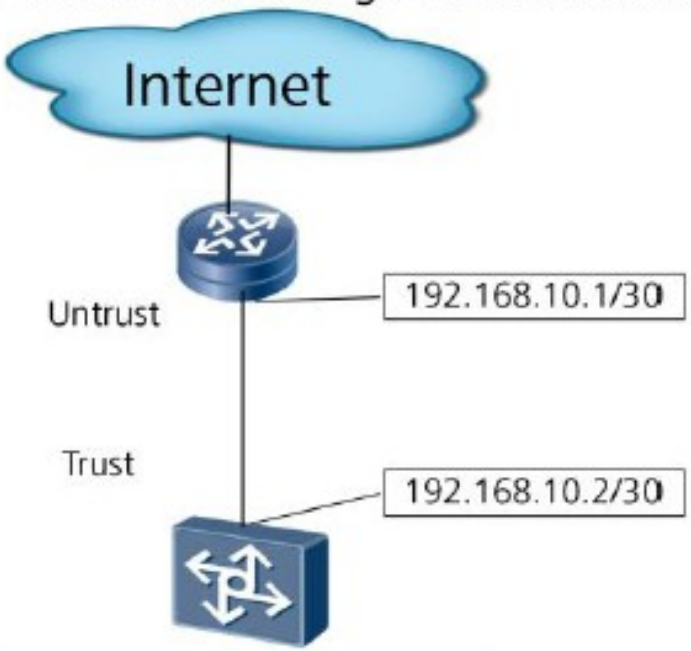


CONCETTI GENERALI DA ESEMPI PARTICOLARI

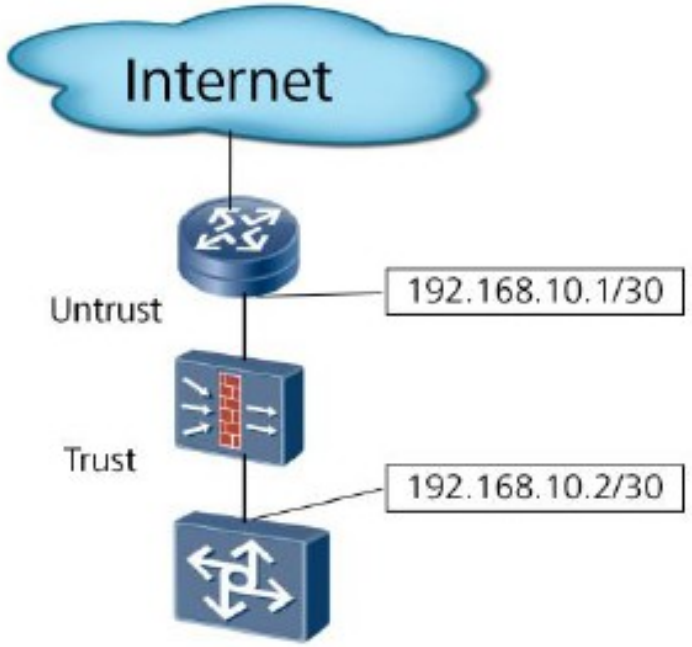
User guide di un paio di vendor...

Firewall Networking – Layer-2 Ethernet Interface

- Networking features
  - Transparent to network topology
  - No need to change the networking



Before Firewall Installation



After Firewall Installation

Copyright © 2015 Huawei Technologies Co., Ltd. All rights reserved.

Modalità

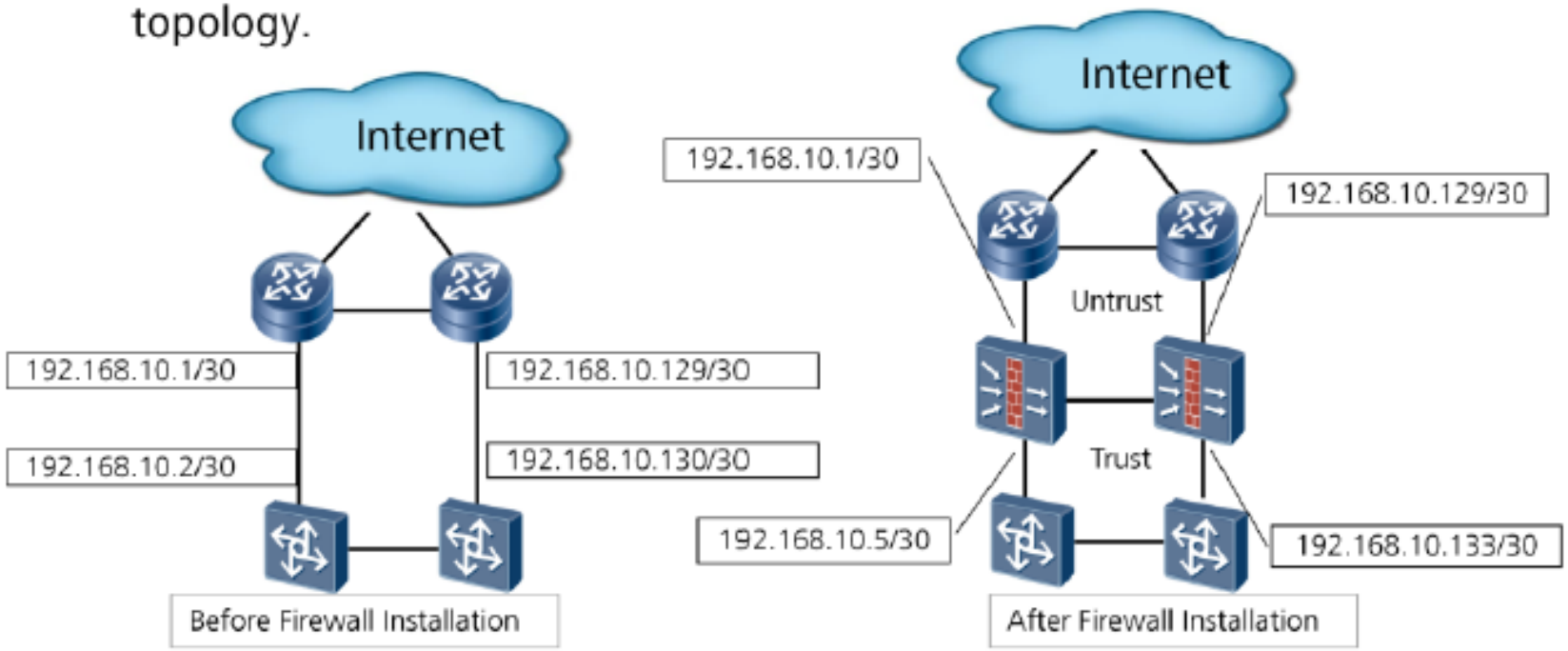
L2 o Transparent

Modalità

L2 o Transparent

Firewall Networking – Layer-3 Ethernet Interface

- Networking features
  - Supports more security features.
  - Has some influence on the network topology.



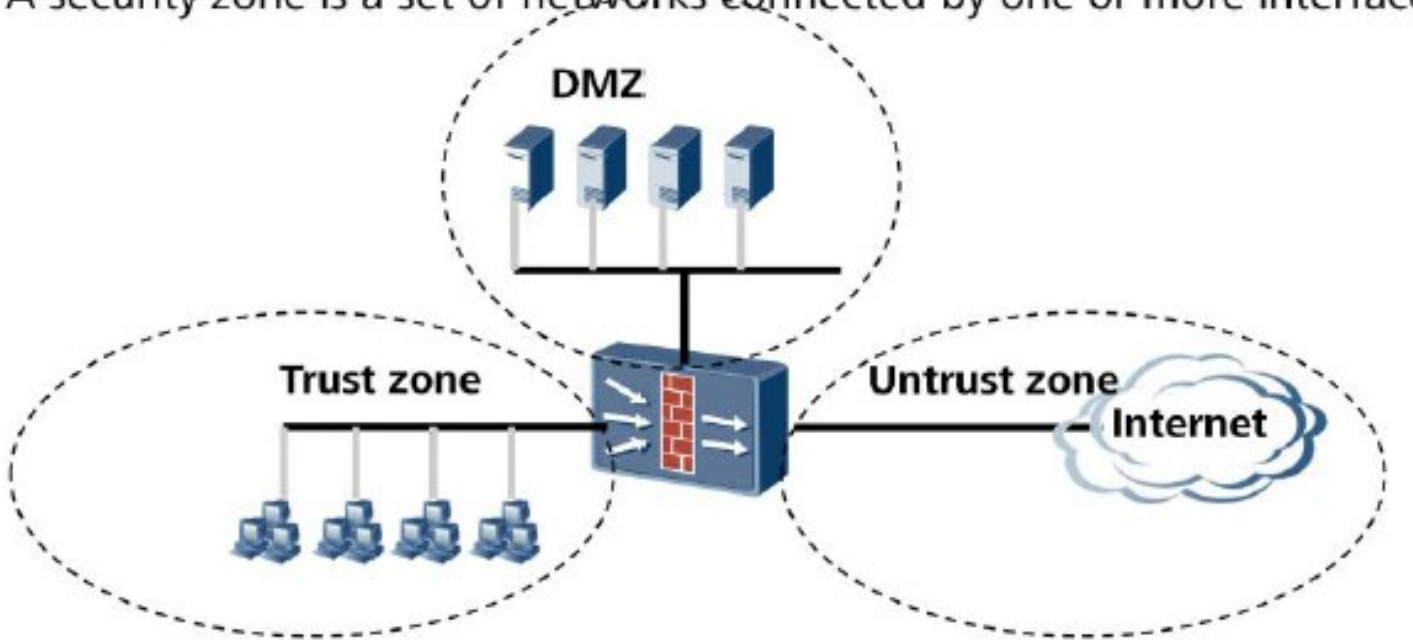
Copyright © 2015 Huawei Technologies Co., Ltd. All rights reserved.

Modalità

L3 o Routed

What Is a Security Zone

- Security zone (Zone)
  - A security zone (also named zone) is a local logical security area, based on which most security policies are implemented.
  - A security zone is a set of networks connected by one or more interfaces.



Copyright © 2015 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Security zone

Security policies implemented on the basis of ***security zones***

Within a zone ***no security policy*** required

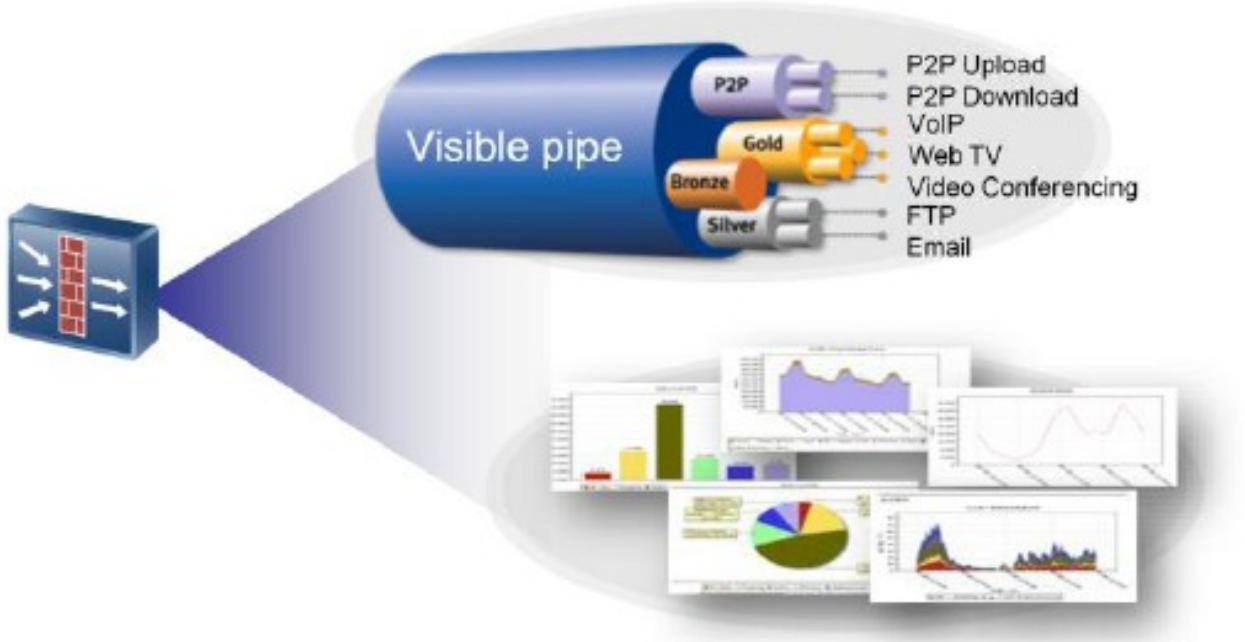
Data exchange *between zones* triggers ***security checks***

Within a firewall:

- devices on the **same interface** reside in the **same security zone**
- one **security zone** can include networks connected to **multiple**

Application Control

- Service Awareness (SA) uses the SA knowledge base to inspect data flows (P2P, VoIP, and video data) in depth, identifies almost all application-layer services, and controls the traffic of the specified types, including allowing and blocking packets, limiting the connection number, and rate limiting.



Copyright © 2015 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Service Awareness

SA inspects application-layer data (layers above UDP/TCP IP)

Firewall rules match application-layer data **to signatures**

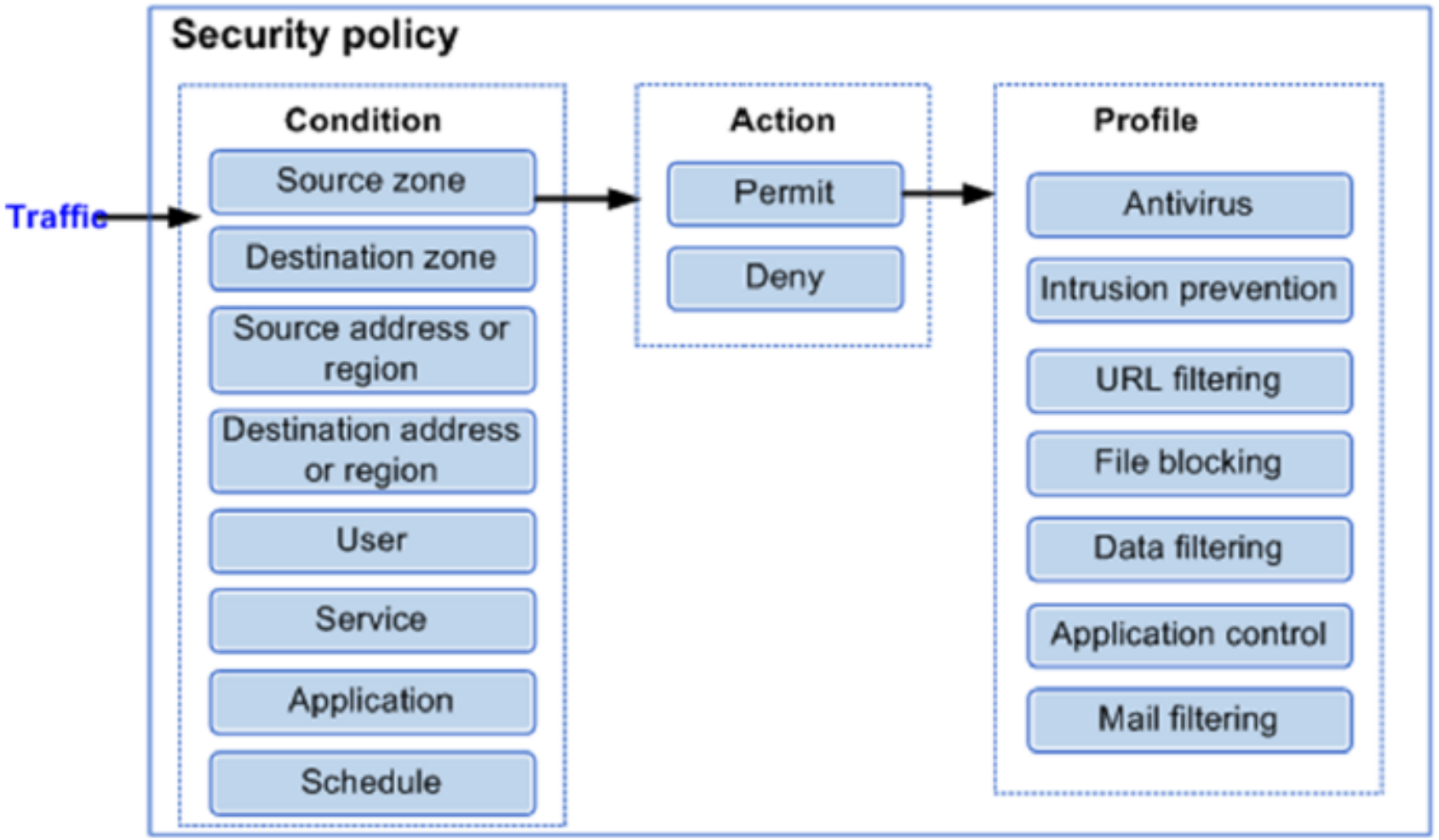
SA **signature database** contains signatures of relevant applications

A rule matching triggers **control actions**

Examples of control actions:

- allow/block traffic
- limit traffic rate

Procedure of Security Policies (1)



Copyright © 2015 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

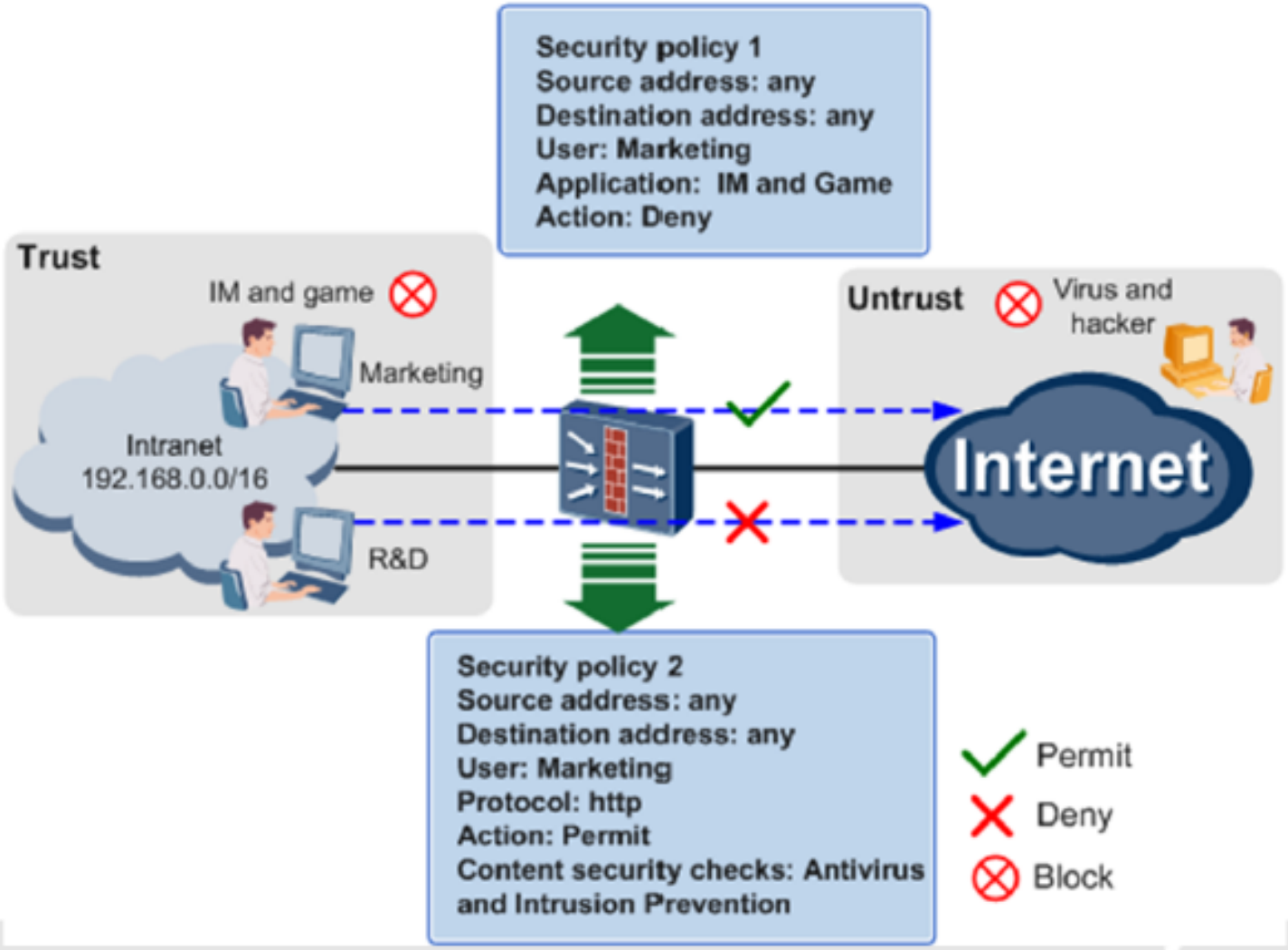
Security Policies

If certain profiles are referenced in the policy and the action defined in the policy is **permit**, the NGFW performs **integrated checks**

The integrated check **inspects the content** carried over the traffic based on the **conditions defined in** the referenced **profiles** and **implements** appropriate **actions**

If any profile check result determines to **block** the traffic, the NGFW blocks the traffic. If all profiles determine to permit the traffic, the traffic through

Procedure of Security Policies (2)

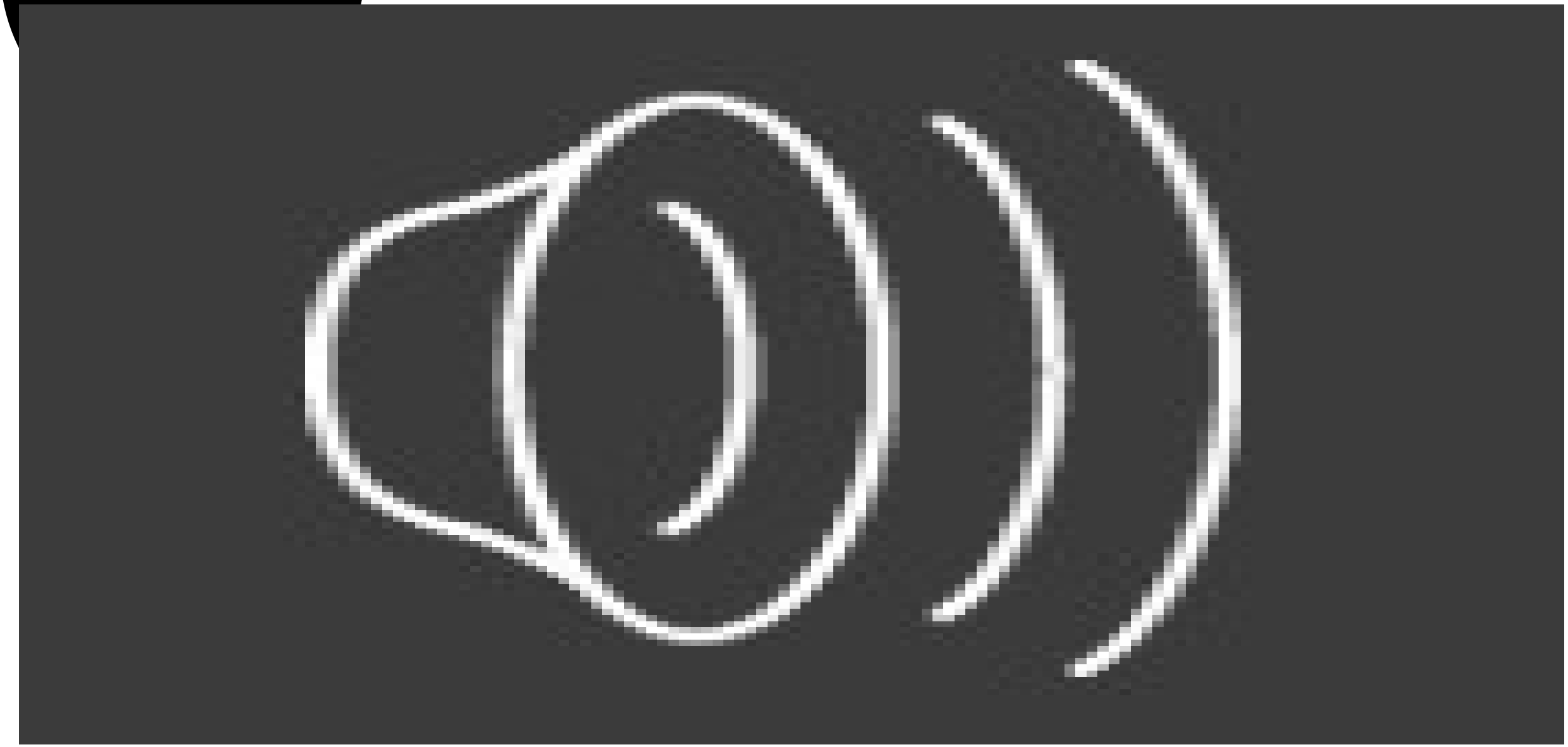


Copyright © 2015 Huawei Technologies Co., Ltd. All rights reserved.

NGFW vs Traditional FW

Security policies of next generation firewalls:

- **Distinguish** among **users** of different departments based on users
- **Distinguish** among various **applications** carried over the same protocol
- Implement **content security check** to block viruses and hacker intrusions



DOMANDA

MA SE I DISPOSITIVI FIREWALL NG FANNO TUTTE QUESTE BELLE COSE PERCHE’ NON LI UTILIZZIAMO ?

Perchè come spesso accade la complessità porta anche alcune limitazioni

NGFW

I dispositivi FIREWALL NG hanno alcune peculiarità

“COSTO”

Dovendo gestire operazioni complesse sui flussi sono dotati di HW costosi

Il software che li gestisce necessità di aggiornamenti in real-time a pagamento

“LENTEZZA”

Dovendo gestire operazioni complesse sui flussi sono molto più lenti di switch e router

“SCARSA SCALABILITA’ ”

A causa delle peculiarita’ a lato sono tipicamente poco scalabili

MISURE

Come possiamo valutare prestazioni, costi e la loro relazione?

Ci affidiamo a laboratori accreditati

oppure... ci proviamo da soli

ICSA labs
A DIVISION OF TRUSECURE CORPORATION

ICSA Labs Firewall Testing
An In Depth Analysis

by

Jack Walsh
Senior Security Engineer
ICSA Labs, a division of TruSecure Corporation

June 10, 2004



Interested in learning more about security?

SANS Institute
InfoSec Reading Room
This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Real-World Testing of Next-Generation Firewalls

Copyright SANS Institute
Author Retains Full Rights

NSS LABS

TEST METHODOLOGY

Next Generation Firewall (NGFW)

v7.0

CERTIFICAZIONI

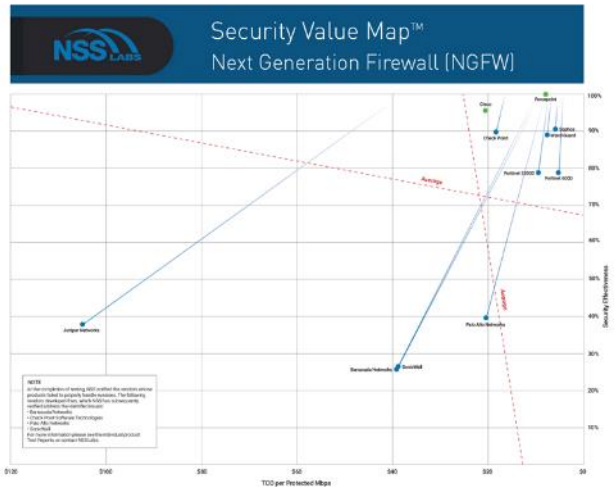
Gli stessi laboratori accreditati producono report comparativi periodici e alcuni anche classifiche

Questo documento potrebbe essere un buon punto di partenza per una valutazione di dispositivi NGFW !

NSS LABS NGFW 2016

Product	Security Effectiveness		Value in US$ (TCO per Protected Mbps)		Overall Rating
Barracuda Networks F600.E20	92.4%	Below Average	$14	Above Average	Neutral
Check Point 13800 NGFW Appliance	99.6%	Above Average	$25	Above Average	Recommended
Cisco ASA 5585-X SSP-60	96.5%	Above Average	$51	Below Average	Neutral
Cisco FirePOWER Appliance 8350	96.3%	Above Average	$23	Above Average	Recommended
Cyberoam CR2500ING-XP	58.1%	Below Average	$22	Above Average	Neutral
Dell SonicWALL SuperMassive E10800	98.1%	Above Average	$24	Above Average	Recommended
Forcepoint Stonesoft NGFW 1402	97.6%	Above Average	$26	Above Average	Recommended
Fortinet FortiGate 3200D	99.6%	Above Average	$9	Above Average	Recommended
Hillstone Networks SG-6000-E5960	99.0%	Above Average	$6	Above Average	Recommended
Huawei Technologies USG6650	98.1%	Above Average	$7	Above Average	Recommended
Juniper Networks SRX5400E	98.0%	Above Average	$97	Below Average	Neutral
Palo Alto Networks PA-7050	95.9%	Above Average	$31	Below Average	Neutral
WatchGuard Technologies XTM 1525	87.7%	Below Average	$18	Above Average	Neutral

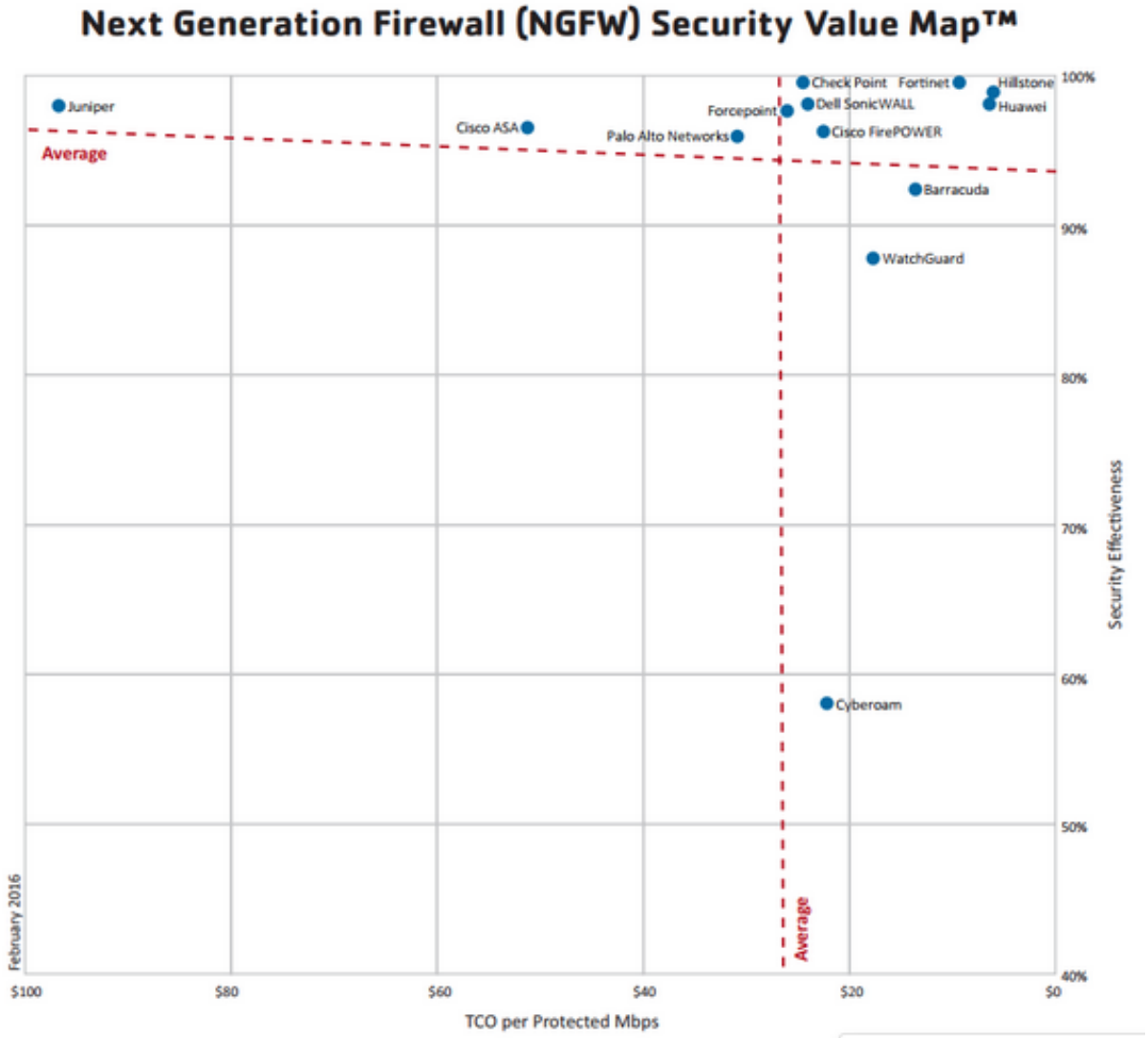
Figure 2 – NSS Labs' 2016 Recommendations for Next Generation Firewall (NGFW)

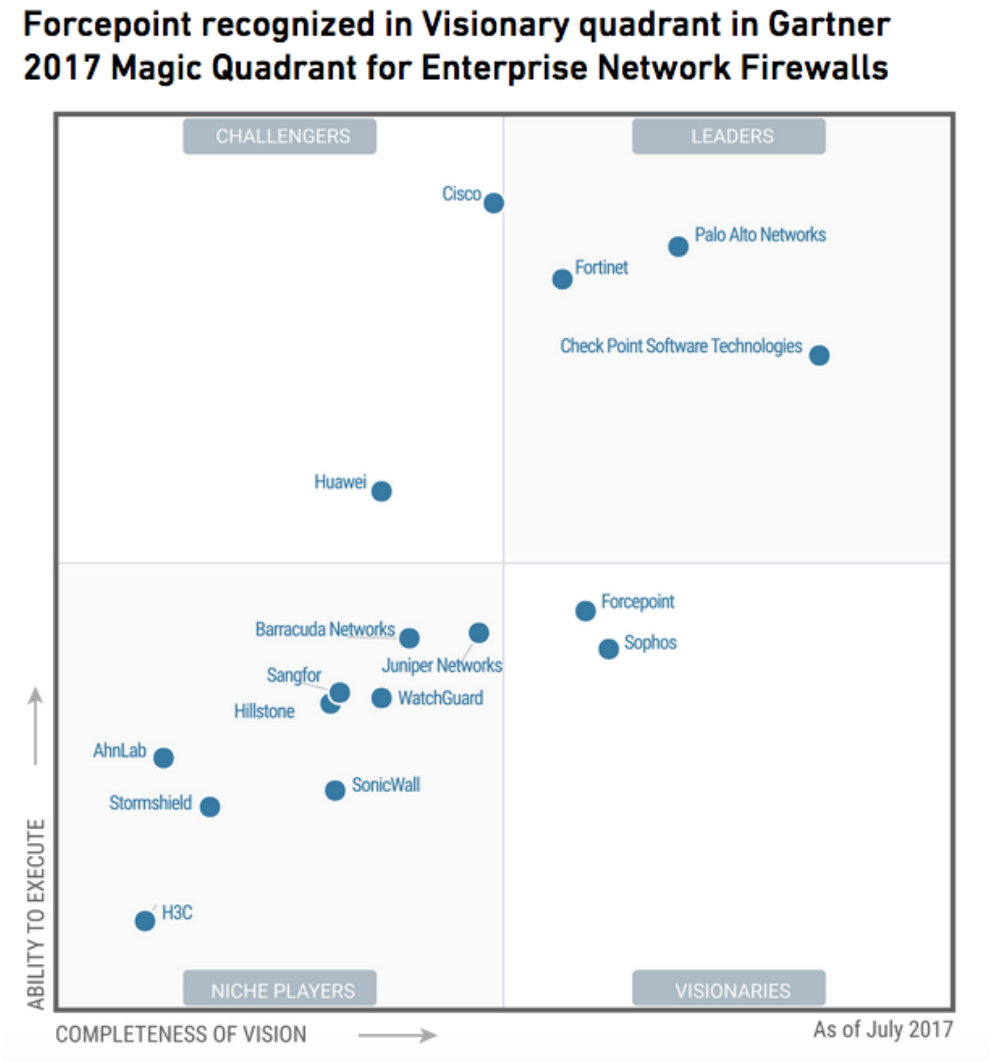


ICSA labs CERTIFIED FIREWALL - CORPORATE

REPORT

…ma sicuramente il più accreditato *(da chi?)* è il Gartner report





	FG-500D	FG-500E	FG-600D	FG-800D	FG-1000D
Firewall Throughput (1518/512/64 byte UDP)	16 / 16 /16 Gbps	36 / 36 / 32 Gbps	36 / 36 / 24 Gbps	36 / 36 / 22 Gbps	52 / 52 / 33 Gbps
Firewall Latency	3 µs	2 µs	3 µs	3 µs	3 µs
Concurrent Sessions	6 Million	8 Million	5.5 Million	5 Million	11 Million
New Sessions/Sec	250,000	300,000	270,000	280,000	280,000
Firewall Policies	10,000	10,000	10,000	10,000	100,000
IPsec VPN Throughput (512 byte) [1]	14 Gbps	20 Gbps	20 Gbps	20 Gbps	25 Gbps
Max G/W to G/W IPSEC Tunnels	2,000	2,000	2,000	2,000	20,000
Max Client to G/W IPSEC Tunnels	50,000	50,000	50,000	50,000	100,000
SSL VPN Throughput	400 Mbps	5 Gbps	2.2 Gbps	2.2 Gbps	3.6 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	500	500	5,000	5,000	10,000
IPS Throughput [1] (HTTP / Enterprise Mix)	5.7 / 3.5 Gbps	11 / 5.2 Gbps	7 / 4 Gbps	8 / 4.2 Gbps	9 / 6 Gbps
SSL Inspection Throughput (IPS, HTTP) [3]	3 Gbps	6.8 Gbps	3.5 Gbps	4 Gbps	4 Gbps
Application Control Throughput (HTTP 64K) [2]	7.5 Gbps	14 Gbps	9 Gbps	9 Gbps	14 Gbps
NGFW Throughput [2, 4]	2.5 Gbps	5 Gbps	3.8 Gbps	4 Gbps	5 Gbps
Threat Protection Throughput [2, 5]	2 Gbps	4.7 Gbps	3 Gbps	3 Gbps	4 Gbps
Max FortiAPs (Total, Tunnel)	512 / 256	512 / 256	1024 / 512	1,024 / 512	4,096 / 1,024
Max FortiSwitches	48	48**	64	64	128
Max FortiTokens	1,000	1,000	1,000	1,000	5,000
Max Registered Endpoints	2,000	2,000	2,000	2,000	20,000
Virtual Domains (Default/Max)	10 / 10	10 / 10	10 / 10	10 / 10	10 / 250
Interfaces	10x GE RJ45, 8x GE SFP	2x 10 GE SFP+, 10x GE RJ45, 8x GE SFP	2x 10 GE SFP+, 10x GE RJ45, 8x GE SFP	2x 10 GE SFP+, 8x GE SFP, 4x GE RJ45 Bypass, 22x GE RJ45	2x 10 GE SFP+, 16x GE SFP, 18x GE RJ45
Local Storage	120 GB	—	120 GB	240 GB	256 GB
Power Supplies	Single AC PS, opt. Ext RPS	Single AC PS, opt. Dual PS	Single AC PS, opt. Ext RPS	Single AC PS, opt. Dual PS	Dual PS
Form Factor	1 RU	1 RU	1 RU	1 RU	2 RU
Variants	LENC	—	LENC	—	LENC

Datas et

per

Model	USG6650	USG6660	USG6670	USG6680
IPv4 Firewall Throughput[1] (1518/512/64-byte, UDP)	20/20/8 Gbit/s	25/25/8 Gbit/s	35/35/8 Gbit/s	40/35/8 Gbit/s
IPv6 Firewall Throughput[1] (1518/512/84-byte, UDP)	20/20/8 Gbit/s	25/25/8 Gbit/s	35/35/8 Gbit/s	40/35/8 Gbit/s
Firewall Throughput (Packets Per Second)	12 Mpps	12 Mpps	12 Mpps	12 Mpps
Firewall Latency (64-byte, UDP)	16 µs	16 µs	16 µs	16 µs
FW + SA* Throughput[2]	15 Gbit/s	18 Gbit/s	19 Gbit/s	20 Gbit/s
FW + SA* Throughput (Realworld)[3]	11 Gbit/s	12 Gbit/s	13 Gbit/s	18 Gbit/s
FW + SA + IPS Throughput[2]	8.8 Gbit/s	8.8 Gbit/s	8.8 Gbit/s	15 Gbit/s
FW + SA + Antivirus Throughput[2]	8 Gbit/s	8 Gbit/s	8 Gbit/s	13 Gbit/s
FW + SA + IPS + Antivirus + URL Throughput[2]	6 Gbit/s	7 Gbit/s	8 Gbit/s	13 Gbit/s
FW + SA + IPS + Antivirus Throughput (Realworld)[3]	5 Gbit/s	5.5 Gbit/s	6 Gbit/s	11 Gbit/s
Concurrent Sessions (HTTP1.1)[1]	8,000,000	10,000,000	10,000,000	12,000,000
New Sessions/Second (HTTP1.1)[1]	300,000	350,000	400,000	400,000
IPsec VPN Throughput[1] (AES-128 + SHA1, 1420-byte)	15 Gbit/s	18 Gbit/s	18 Gbit/s	18 Gbit/s

	FG-500D
Firewall Throughput (1518/512/64 byte UDP)	16 / 16 /16 Gbps
Firewall Latency	3 µs
Concurrent Sessions	6 Million
New Sessions/Sec	250,000
Firewall Policies	10,000
IPsec VPN Throughput (512 byte) [1]	14 Gbps
Max G/W to G/W IPSEC Tunnels	2,000
Max Client to G/W IPSEC Tunnels	50,000
SSL VPN Throughput	400 Mbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	500
IPS Throughput [1] (HTTP / Enterprise Mix)	5.7 / 3.5 Gbps
SSL Inspection Throughput (IPS, HTTP) [3]	3 Gbps
Application Control Throughput (HTTP 64K) [2]	7.5 Gbps
NGFW Throughput [2,4]	2.5 Gbps
Threat Protection Throughput [2,5]	2 Gbps
Max FortiAPs (Total, Tunnel)	512 / 256
Max FortiSwitches	48
Max FortiTokens	1,000
Max Registered Endpoints	2,000
Virtual Domains (Default/Max)	10 / 10
Interfaces	10x GE RJ45, 8x GE SFP
Local Storage	120 GB
Power Supplies	Single AC PS, opt. Ext RPS
Form Factor	1 RU
Variants	LENC

	PA-5260	PA-5250	PA-5220
	72.2 Gbps	35.9 Gbps	18.5 Gbps
	30 Gbps	20.3 Gbps	9.2 Gbps
	21 Gbps	14 Gbps	5 Gbps
	468,000	348,000	169,000
	32,000,000	8,000,000	4,000,000
	25/225	25/125	10/20
	PA-5260	PA-5250	PA-5220
SFP+ SFP, (24)	(4) 100/1000/10G Cu, (16) 1G/10G SFP/SFP+, (4) 40G/100G QSFP28		(4) 100/1000/10G Cu, (16) 1G/10G SFP/SFP+, (4) 40G QSFP+
of-band	(2) 10/100/1000 Cu, (1) 10/100/1000 out-of-band management, (1) RJ45 console		
	(1) 40G/100G QSFP28 HA		(1) 40G QSFP+ HA
14U, 19" Airduct kit	3U, 19" standard rack		
2700W)	2x1200W AC or DC (1:1 Fully Redundant)		
	Yes		
	System: 240GB SSD, RAID1; Log: 2TB HDD, RAID1		
	Yes		

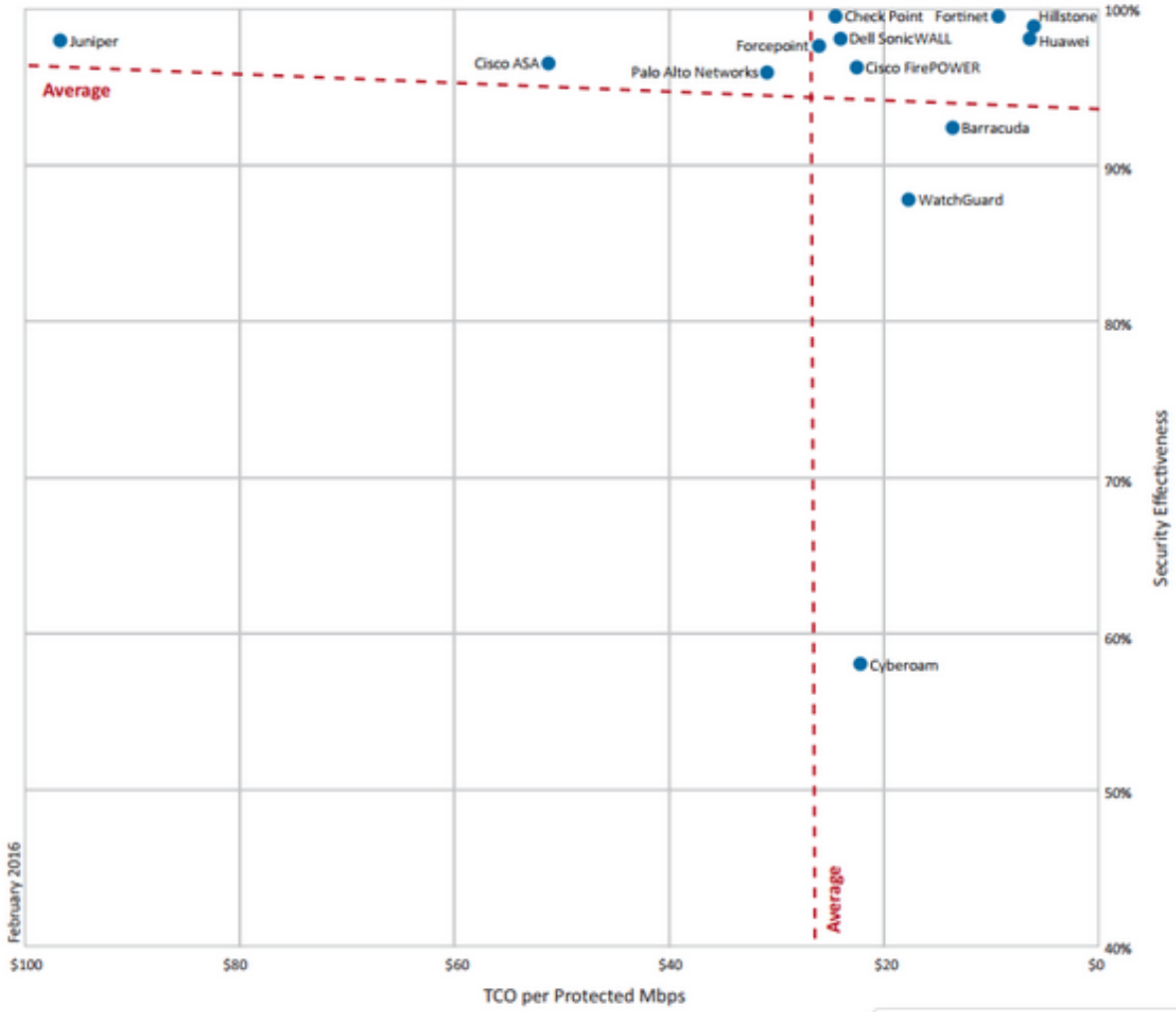
-5020	PA-3060	PA-3050	PA-3020
Gbps	4 Gbps	4 Gbps	2 Gbps
Gbps	2 Gbps	2 Gbps	1 Gbps
Gbps	500 Mbps	500 Mbps	500 Mbps
0,000	50,000	50,000	50,000
00,000	500,000	500,000	250,000
0/20	1/6	1/6	1/6
-5020	PA-3060	PA-3050	PA-3020
1000, (8) SFP	(8) 10/100/1000, (8) SFP, (2) 10 SFP+	(12) 10/100/1000, (8) SFP	
ment, (1) RJ45	(1) 10/100/1000 out-of-band management,(2) 10/100/1000 high availability, (1) RJ-45 console		
	1.5U, 19" standard rack	1U, 19" standard rack	
	Redundant 400W AC	250W AC	
	Yes	No	
	120GB SSD		
	No		

Performance and Capacities[1]	PA-7080 System[2]	PA-7050 System[2]	PA-5260	PA-5250	PA-5220
Firewall throughput (App-ID)	200 Gbps	120 Gbps	72.2 Gbps	35.9 Gbps	18.5 Gbps
Threat prevention throughput	100 Gbps	60 Gbps	30 Gbps	20.3 Gbps	9.2 Gbps
IPSec VPN throughput	80 Gbps	48 Gbps	21 Gbps	14 Gbps	5 Gbps
New sessions per second	1,200,000	720,000	458,000	348,000	169,000
Max sessions	40,000,000/80,000,000[3]	24,000,000/48,000,000[3]	32,000,000	8,000,000	4,000,000
Virtual systems (base/max[2])	25/225	25/225	25/225	25/125	10/20
Hardware Specifications	**PA-7080 System**	**PA-7050 System**	**PA-5260**	**PA-5250**	**PA-5220**
Interfaces supported NPC option 1[4]	Up to (20) QSFP+, (120) SFP+	Up to (12) QSFP+, (72) SFP+	(4) 100/1000/10G Cu, (16) 1G/10G SFP/SFP+, (4) 40G/100G QSFP28		(4) 100/1000/10G Cu, (16) 1G/10G SFP/SFP+, (4) 40G QSFP+
Interfaces supported NPC option 2[4]	Up to (120) 10/100/1000, (80) SFP, (40) SFP+	Up to (72) 10/100/1000, (48) SFP, (24) SFP+			
Management I/O	(2) 10/100/1000, (2) QSFP+ high availability, (1) 10/100/1000 out-of-band management, (1) RJ45 console		(2) 10/100/1000 Cu, (1) 10/100/1000 out-of-band management, (1) RJ45 console		
			(1) 40G/100G QSFP28 HA		(1) 40G QSFP+ HA
Rack mountable?	19U, 19" standard rack	9U, 19" standard rack or 14U, 19" standard rack with optional Airduct kit	3U, 19" standard rack		
Power supply	4x2500W AC (2400W / 2700) expandable to 8	4x2500W AC (2400W / 2700W)	2x1200W AC or DC (1:1 Fully Redundant)		
Redundant power supply?	Yes		Yes		
Disk drives	2TB RAID1		System: 240GB SSD, RAID1. Log: 2TB HDD, RAID1		
Hot swap fans	Yes		Yes		

Performance and Capacities[1]	PA-5060	PA-5050	PA-5020	PA-3060	PA-3050	PA-3020
Firewall throughput (App-ID)	20 Gbps	10 Gbps	5 Gbps	4 Gbps	4 Gbps	2 Gbps
Threat prevention throughput	10 Gbps	5 Gbps	2 Gbps	2 Gbps	2 Gbps	1 Gbps
IPSec VPN throughput	4 Gbps	4 Gbps	2 Gbps	500 Mbps	500 Mbps	500 Mbps
New sessions per second	120,000	120,000	120,000	50,000	50,000	50,000
Max sessions	4,000,000	2,000,000	1,000,000	500,000	500,000	250,000
Virtual systems (base/max[2])	25/225	25/125	10/20	1/6	1/6	1/6
Hardware Specifications	**PA-5060**	**PA-5050**	**PA-5020**	**PA-3060**	**PA-3050**	**PA-3020**
Interfaces supported[4]	(12) 10/100/1000, (8) SFP, (4) 10 SFP+		(12) 10/100/1000, (8) SFP	(8) 10/100/1000, (8) SFP, (2) 10 SFP+	(12) 10/100/1000, (8) SFP	
Management I/O	(2) 10/100/1000 high availability, (1) 10/100/1000 out-of-band management, (1) RJ45 console			(1) 10/100/1000 out-of-band management,(2) 10/100/1000 high availability, (1) RJ-45 console		
Rack mountable?	2U, 19" standard rack			1.5U, 19" standard rack	1U, 19" standard rack	
Power supply	Redundant 450W AC or DC			Redundant 400W AC	250W AC	
Redundant power supply?	Yes			Yes	No	
Disk drives	120GB or 240GB SSD, RAID Optional			120GB SSD		
Hot swap fans	Yes			No		

View Cart

Next Generation Firewall (NGFW) Security Value Map™



	Price:	Qty:	Item Total:
8x5 FortiCare and FortiGuard UTM Protection	$27,900.00	1	$27,900.00

1 item: **$27,900.00**

Update Cart | Empty Cart

$ 45,455.99
Advertised Price

Lease Option ($1,229.58 /month)

llability: 8–10 days

s placed today will ship within 10 days

urity appliance

-mountable

More

921.00

386.00

Cart -OR- Continue Shopping

otal US$17,713.00

al US$17,713.00

Add All Items To Cart

Sign In to Email this page or Save as Favorite

Ce li possiamo permettere

!

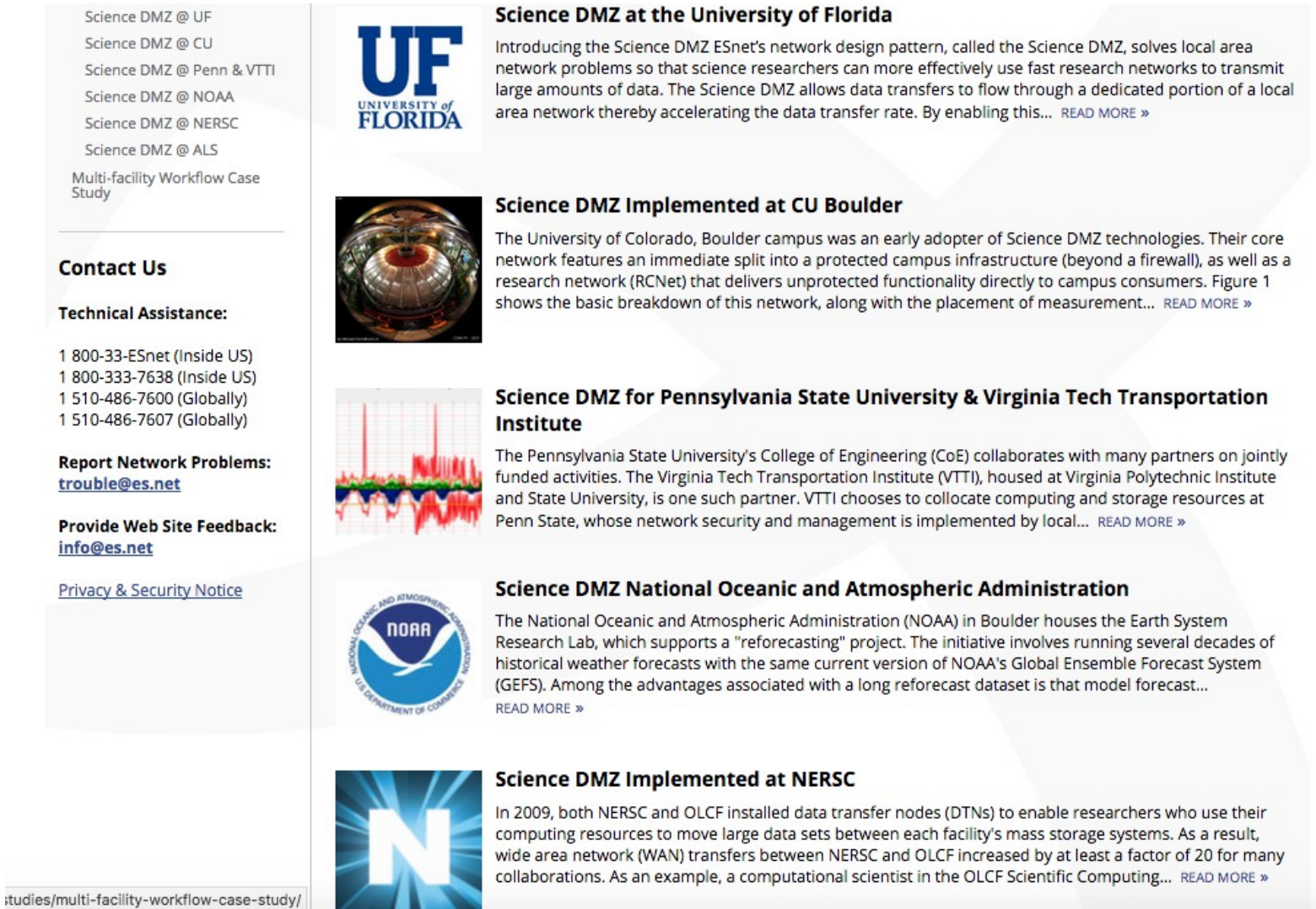
?

La comunità della ricerca è sempre in carenza di fondi

...ma nell'era dei Big Data ha tanti dati da proteggere

THE SCIDMZ

Science high throughput data stream with no Firewall



- Science DMZ @ UF
- Science DMZ @ CU
- Science DMZ @ Penn & VTTI
- Science DMZ @ NOAA
- Science DMZ @ NERSC
- Science DMZ @ ALS
- Multi-facility Workflow Case Study

Contact Us

Technical Assistance:

1 800-33-ESnet (Inside US)
1 800-333-7638 (Inside US)
1 510-486-7600 (Globally)
1 510-486-7607 (Globally)

Report Network Problems:
trouble@es.net

Provide Web Site Feedback:
info@es.net

Privacy & Security Notice

studies/multi-facility-workflow-case-study/

Science DMZ at the University of Florida

Introducing the Science DMZ ESnet's network design pattern, called the Science DMZ, solves local area network problems so that science researchers can more effectively use fast research networks to transmit large amounts of data. The Science DMZ allows data transfers to flow through a dedicated portion of a local area network thereby accelerating the data transfer rate. By enabling this... READ MORE »

Science DMZ Implemented at CU Boulder

The University of Colorado, Boulder campus was an early adopter of Science DMZ technologies. Their core network features an immediate split into a protected campus infrastructure (beyond a firewall), as well as a research network (RCNet) that delivers unprotected functionality directly to campus consumers. Figure 1 shows the basic breakdown of this network, along with the placement of measurement... READ MORE »

Science DMZ for Pennsylvania State University & Virginia Tech Transportation Institute

The Pennsylvania State University's College of Engineering (CoE) collaborates with many partners on jointly funded activities. The Virginia Tech Transportation Institute (VTTI), housed at Virginia Polytechnic Institute and State University, is one such partner. VTTI chooses to collocate computing and storage resources at Penn State, whose network security and management is implemented by local... READ MORE »

Science DMZ National Oceanic and Atmospheric Administration

The National Oceanic and Atmospheric Administration (NOAA) in Boulder houses the Earth System Research Lab, which supports a "reforecasting" project. The initiative involves running several decades of historical weather forecasts with the same current version of NOAA's Global Ensemble Forecast System (GEFS). Among the advantages associated with a long reforecast dataset is that model forecast...
READ MORE »

Science DMZ Implemented at NERSC

In 2009, both NERSC and OLCF installed data transfer nodes (DTNs) to enable researchers who use their computing resources to move large data sets between each facility's mass storage systems. As a result, wide area network (WAN) transfers between NERSC and OLCF increased by at least a factor of 20 for many collaborations. As an example, a computational scientist in the OLCF Scientific Computing... READ MORE »

The Science DMZ: A Network Design Pattern for Data-Intensive Science

Eli Dart
Energy Sciences Network
Lawrence Berkeley National Laboratory
Berkeley, CA 94720
eddart@lbl.gov

Lauren Rotman
Energy Sciences Network
Lawrence Berkeley National Laboratory
Berkeley, CA 94720
lbrotman@lbl.gov

Brian Tierney
Energy Sciences Network
Lawrence Berkeley National Laboratory
Berkeley, CA 94720
bltierney@lbl.gov

Mary Hester
Energy Sciences Network
Lawrence Berkeley National Laboratory
Berkeley, CA 94720
mchester@lbl.gov

Jason Zurawski
Internet2
Office of the CTO
Washington DC, 20036
zurawski@internet2.edu

Abstract

The ever-increasing scale of scientific data has become a significant challenge for researchers that rely on networks to interact with remote computing systems and transfer results to collaborators worldwide. Despite the availability of high-capacity connections, scientists struggle with inadequate cyberinfrastructure that cripples data transfer performance, and impedes scientific progress. The *Science DMZ* paradigm comprises a proven set of network design patterns that collectively address these problems for scientists. We explain the Science DMZ model, including network architecture, system configuration, cybersecurity, and performance tools, that creates an optimized network environment for science. We describe use cases from universities, supercomputing centers and research laboratories, highlighting the effectiveness of the Science DMZ model in diverse operational settings. In all, the Science DMZ model is a solid platform that supports any science workflow, and flexibly accommodates emerging network technologies. As a result, the Science DMZ vastly improves collaboration, accelerating scientific discovery.

This manuscript has been authored by an author at Lawrence Berkeley National Laboratory under Contract No. DE-AC02-05CH11231 with the U.S. Department of Energy. The U.S. Government retains, and the publisher, by accepting the article for publication, acknowledges, that the U.S. Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for U.S. Government purposes.

ACM acknowledges that this contribution was authored or co-authored by an employee, contractor or affiliate of the United States government. As such, the Government retains a nonexclusive, royalty-free right to publish or reproduce this article, or to allow others to do so, for Government purposes only. Copyright is held by the owner/author(s). Publication rights licensed to ACM.

SC13 November 17-21, 2013, Denver, CO, USA

Copyright 2013 ACM 978-1-4503-2378-9/13/11 ...$15.00.

http://dx.doi.org/10.1145/2503210.2503245

Categories and Subject Descriptors

C.2.1 [**Computer–Communication Networks**]: Network Architecture and Design; C.2.3 [**Computer–Communication Networks**]: Network Operations—*network management, network monitoring*; C.2.5 [**Computer–Communication Networks**]: Local and Wide-Area Networks—*internet*

General Terms

Performance, Reliability, Design, Measurement

1. INTRODUCTION

A design pattern is a solution that can be applied to a general class of problems. This definition, originating in the field of architecture [1, 2], has been adopted in computer science, where the idea has been used in software designs [6] and in our case network designs. The network design patterns we discuss are focused on high end-to-end network performance for data-intensive science applications. These patterns focus on optimizing the network interactions between wide area networks, campus networks, and computing systems.

The Science DMZ model, as a design pattern, can be adapted to solve performance problems on *any* existing network. Of these performance problems, packet loss has proven to be the most detrimental as it causes an observable and dramatic decrease in data throughput for most applications. Packet loss can be caused by many factors including: firewalls that cannot effectively process science traffic flows; routers and switches with inadequate burst capacity; dirty optics; and failing network and system components. In addition, another performance problem can be the misconfiguration of data transfer hosts, which is often a contributing factor in poor network performance.

Many of these problems are found on the local area networks, often categorized as "general-purpose" networks, that are not designed to support large science data flows. Today many scientists are relying on these network infrastructures to share, store, and analyze their data which is often geographically dispersed.

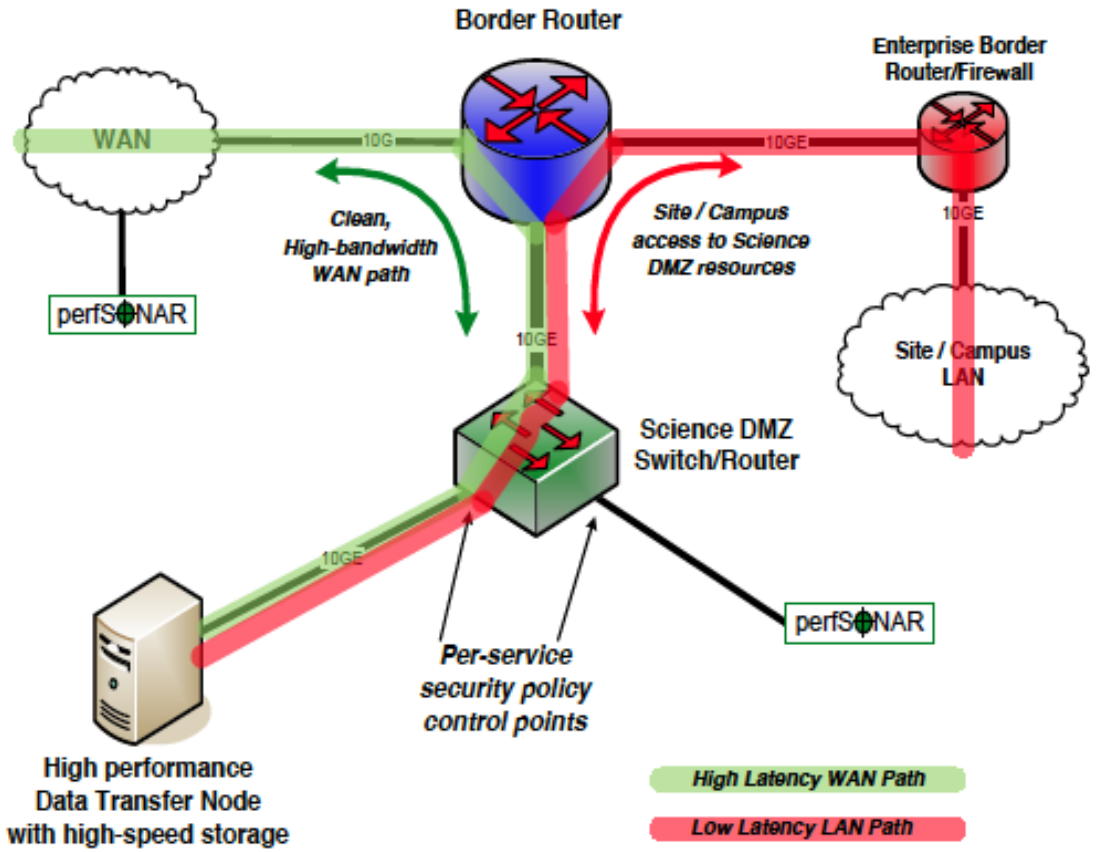


Figure 3: Example of the simple Science DMZ. Shows the data path through the border router and to the DTN (shown in green). The campus site access to the Science DMZ resources is shown in red.

SCIENCE DMZ howto from ESNET

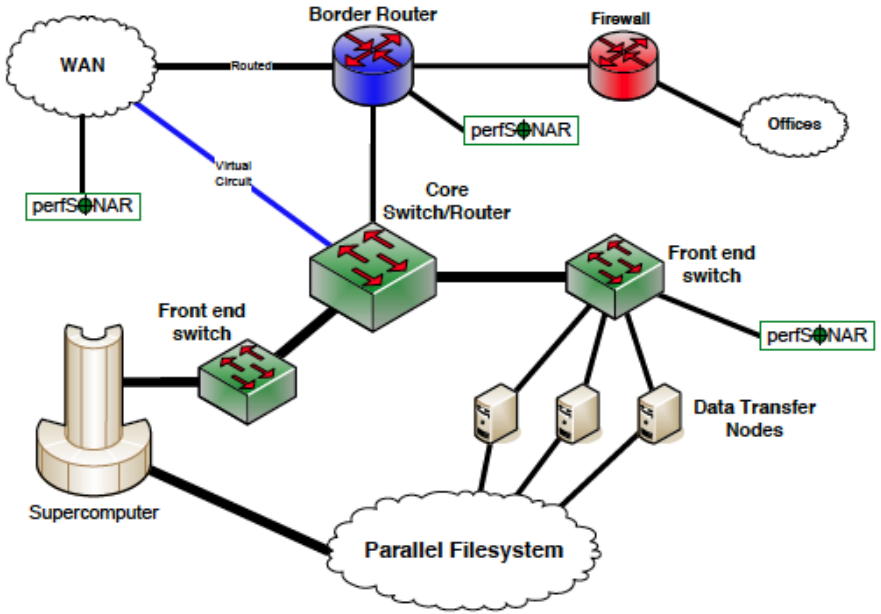


Figure 4: Example supercomputer center built as a Science DMZ.

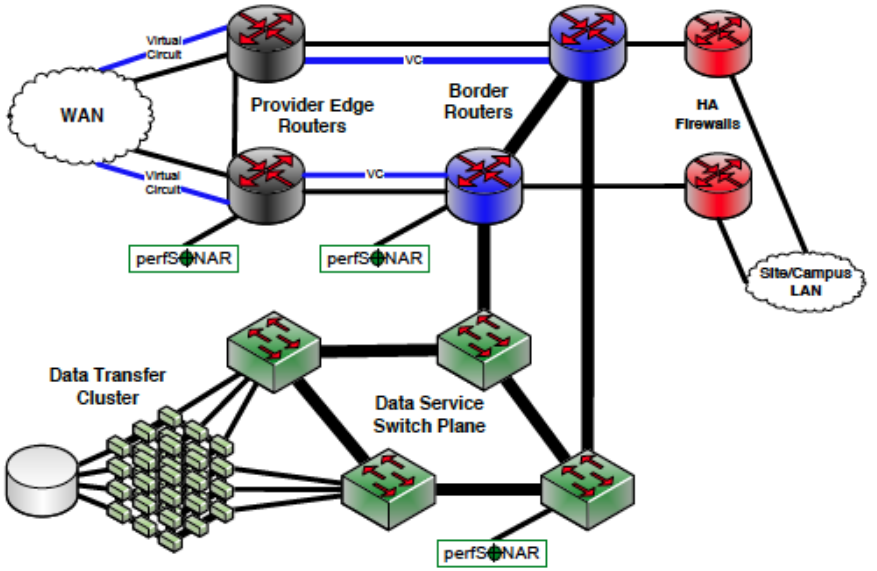


Figure 5: Example of an extreme data cluster. The wide area data path covers the entire network front-end, similar to the supercomputer center model.

https://youtu.be/i2lHQgLBmSE

https://youtu.be/J2IUKKdZIHI

THE END
Q&A

THANK YOU

Gianluca Peco | gianluca.peco@bo.infn.it