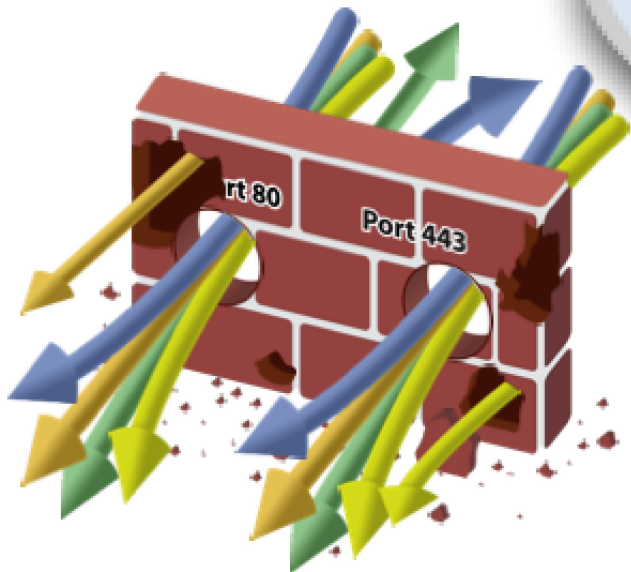


Application Vulnerability Report PaloAlto Networks

Le Applicazioni Cambiano, I Firewalls No

- Il gateway è il miglior posto dove rinforzare le policy di controllo
 - Vede tutto il traffico
 - Definisce trust boundary



- MA .Le applicazioni sono cambiate
 - Ports \neq Applications
 - IP Addresses \neq Users
 - Packets \neq Content

Bisogna ripristinare Visibilità e Controllo nel Firewall

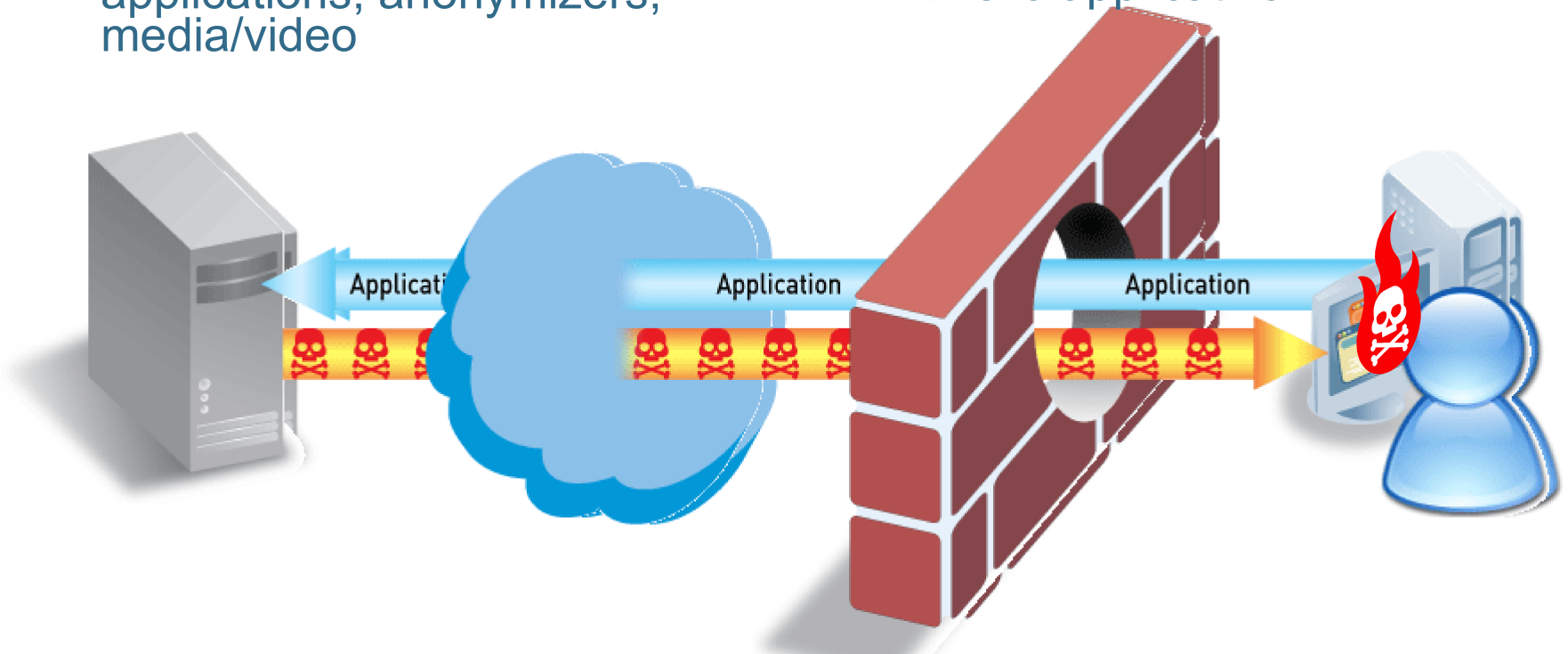
Le Applicazioni Comportano dei Rischi

Le Applicazioni possono essere “minacce”

- P2P file sharing, tunneling applications, anonymizers, media/video

Applicazioni portano minacce

- I Top 20 pericoli SANS– la maggior parte sono minacce a livello applicativo

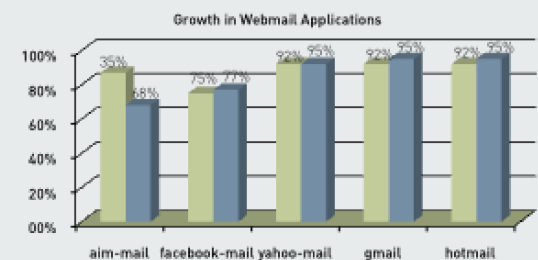
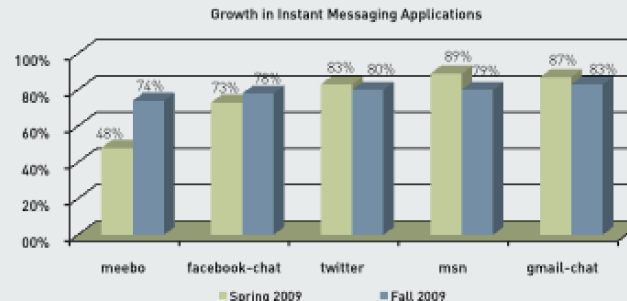
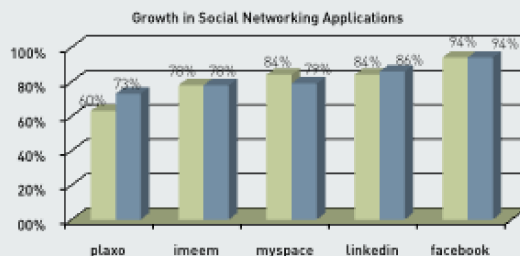
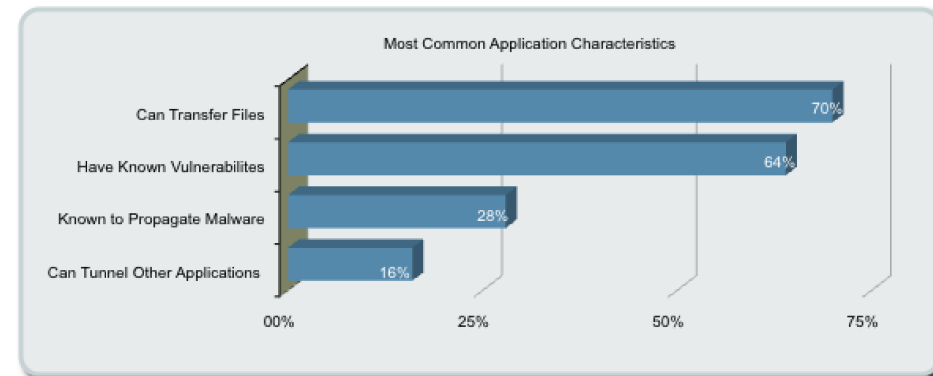


Applicazioni e minacce a livello applicativo sono gli imputati delle maggiori violazioni conosciute : Pfizer, VA, US Army

Applicazioni Enterprise 2.0 e Diffusione dei Rischi

- Palo Alto Networks' Application Usage & Risk Report evidenzia il comportamento effettivo di 1M+ utenti attraverso più di 200 organizzazioni.
 - Applicazioni Enterprise 2.0 – Twitter, Facebook, Sharepoint, e blog/wiki applications – utilizzate in maniera assai diffusa – sia per uso personale sia per business. Facebook estende il dominio dei social networking su IM e webmail
 - Risultati: nonostante tutti abbiano un firewall, e molti utilizzino IPS, proxies, e URL filtering – nessuna di queste organizzazioni può controllare quali applicazioni girano nel loro networks.

Le applicazioni trasportano rischi: business continuity, perdita di dati, compliance, produttività, e costi operativi



Controllo Globale di Applicazioni, Utenti e Contenuti

Application Command Center (ACC)

Vede le applicazioni, URLs, minacce, attività di data filtering

Aggiunge/Rimuove filtri per ottenere i risultati desiderati

The screenshot displays the Palo Alto Networks Application Command Center (ACC) interface. The left sidebar contains navigation tabs: Application, URL Filtering, Threat Prevention, and Data Filtering. The main panel shows the 'Application' view for 'facebook-base'. The 'Application Information' section provides details about Facebook, including its name, related applications, and a description. The 'Top Applications' table lists various applications and their session counts and bytes. The 'Top Sources' table lists source addresses, host names, and users. The 'Top Destinations' table lists destination addresses, host names, and users.

Application Information

Name: facebook-base
Related: facebook
Description: Facebook (branded as "facebook") is a social networking website launched on February 4, 2004. The free privately owned and operated by Facebook, Inc. Users can join networks organized by city, workplace, school, and connect and interact with other people. People can also add friends and send them messages, and update to notify friends about themselves. The website's name refers to the paper facebook depicting member community that some American colleges and preparatory schools give to incoming students, faculty, and staff to know other people on campus. Features include a Wall for posting messages and Photos for uploading digital photos. Facebook has more than 80 million active users worldwide. Facebook has met with some controversy over its privacy policy, which has been blocked in several countries including Syria and Iran. Privacy has also been an issue, and it has been the subject of several lawsuits from users claiming that Facebook stole their source code and other intellectual property.

Container Application: facebook
Standard Ports: tcp/80
Capable of File Transfer: yes
Used by Malware: yes
Excessive Bandwidth Use: no
Evasive: no
Tunnels Other Applications: yes
Additional Information: Wikipedia Google Yahoo!

Top Applications

Risk	Application	Sessions	Bytes
1	web-browsing	300	2,276,586
2	facebook-base	123	698,546
3	facebook-chat	46	209,009
4	dns	26	10,454
5	myspace-base	24	605,456
6	ntp	21	3,870
7	myspace-mail	12	208,662
8	flash	10	368,366
9	myspace-im	8	34,896
10	photobucket	4	38,730
11	myspace-video	4	6,214
12	rtmpe	2	10,766
13	ssl	2	16,702
14	http-audio	2	12,402
15	google-analytics	2	2,334

Top Sources

Source address	Source Host Name	Source User	Bytes	Sessions
1 10.154.1.27	engr27.net1.bigedu.local	pancademo\ellen.cook	4,503,013	586

Top Destinations

Destination address	Destination Host Name	Destination User	Bytes	Sessions
1 69.63.176.161	channel01.01.05.sfp2p.facebook.com		570,079	1
2 198.109.255.76	s198-109-255-76.deploy.akamaitechnologies.com		339,212	1
3 137.145.204.10	ms3.cnn.net		10,454	1
4 216.178.38.202	216.178.38.202		65,610	1

Filter on Facebook-base

Filter on Facebook-base
and user cook

Remove Facebook to
expand view of cook

Mirato a risolvere 3 problemi chiave per il Business

Identificazione e Controllo delle Applicazioni

Visibilità di oltre 1.100 applicazioni, senza l'uso di porte, protocolli, encryption, o tattiche evasive

Controllo capillare sulle applicazioni (allow, deny, limit, scan, shape)

Punta alle carenze delle Infrastrutture chiave dei firewall legacy

Prevenzione delle Minacce

Stop a diverse minacce – exploits (by vulnerability), viruses, spyware

Stop furti di dati confidenziali (e.g., credit card #, social security #)

Motori Stream-based assicurano alte performance

Applica policy di utilizzo sugli utenti per l'uso generico della navigazione su web site

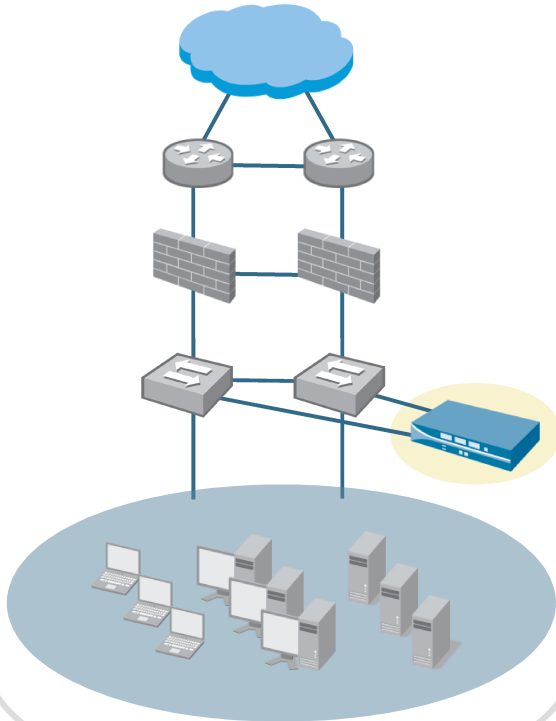
Semplificazione dell'Infrastruttura di Sicurezza

Mette il firewall al centro dell'infrastruttura di sicurezza di rete

Riduce la complessità dell'architettura

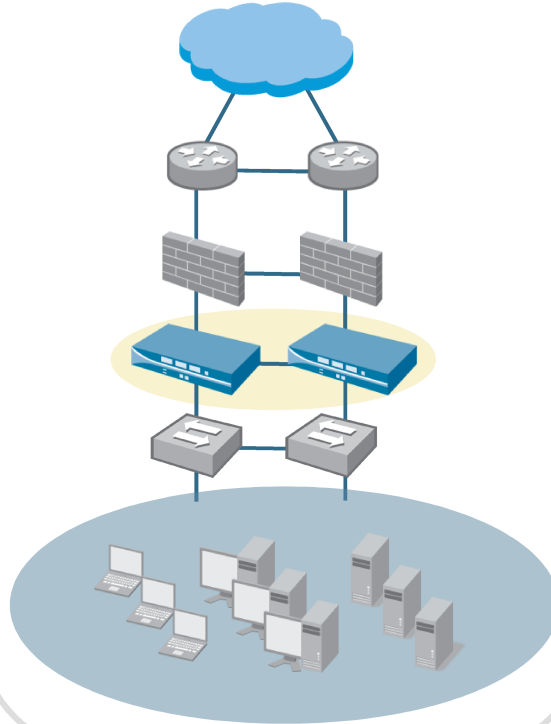
Opzioni di Sviluppo Flessibili

Visibilità delle Applicazioni



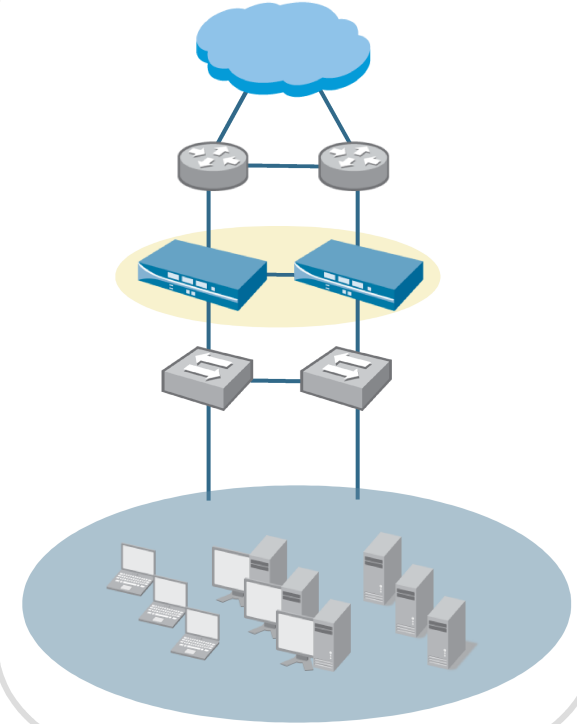
- Connesso alla span port
- Offre visibilità delle applicazioni senza uno sviluppo in linea

Transparent In-Line



- Posizionato trasparentemente dietro firewall esistenti
- Offre application visibility & control senza modificare il networking

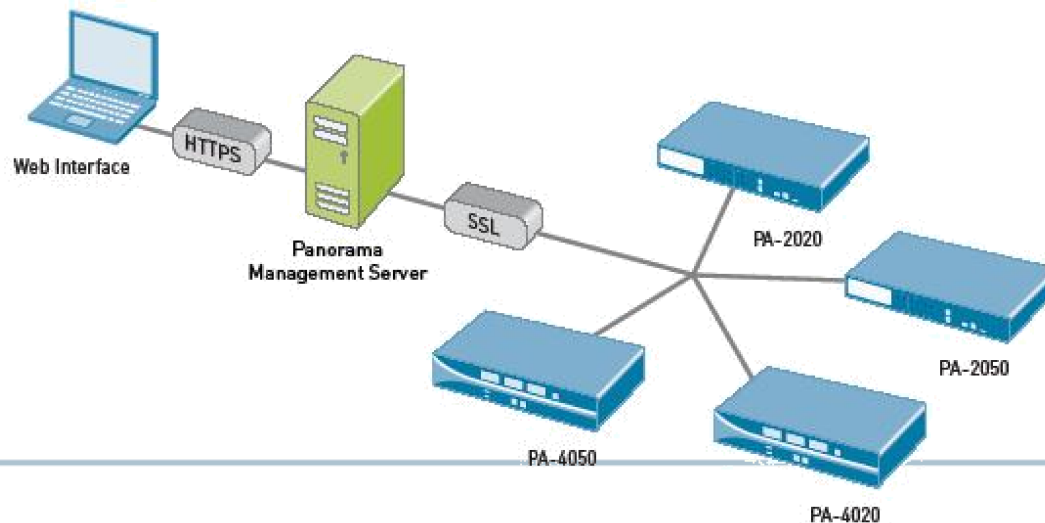
Sostituzione di Firewall



- Rimpiazza firewall esistenti
- Offre visibilità e controllo delle applicazioni e della rete di base, consolida le policy, ad alte prestazioni

Dispositivi Aziendali e Gestione delle policy

- Gestione intuitiva e flessibile
 - CLI, Web, Panorama, SNMP, Syslog
- PANORAMA, applicazione di gestione centralizzata
 - Consolidamento della gestione, logging, e monitoring dei dispositivi Palo Alto Networks
 - Interfaccia Web logica tra Panorama e I device UI
 - Network-wide ACC/monitoring views, log collection, reporting
- Tutte le interfacce lavorano nella configurazione attuale, evitando problemi di sincronia



Visibilità delle Applicazioni degli Utenti e dei Contenuti



Edit Application In Rule -- Web Page Dialog

any
select

Search

334 matching applications (Clear Filters)

Filters

Type here...

Add Filter >>

Selected Filters

Selected Applications

Groups

-- Choose a group --

Add Group >>

Category	Subcategory	Technology	Risk	Characteristic
business-systems	auth-service	41 browser-based	179	107 Vulnerabilities
collaboration	database	121 client-server	13	35 Prone to Misuse
general-internet	encrypted-tunnel	110 network-protocol	46	139 Widely used
media	erp-crm	4 peer-to-peer	17	20 Excessive Bandwidth
networking	general-business		25	100 Transfers Files
unknown	infrastructure			53 Evasive
	ip-protocol			4 Used by Malware
	ip-management			11 Tunnels Other Apps

Name	Shared	Category	Subcategory	Risk	Technology
3pc	✓	networking	ip-protocol	1	network-protocol
active-directory	✓	business-systems	auth-service	2	client-server
activenet	✓	networking	ip-protocol	1	network-protocol
afp	✓	business-systems	storage-backup	1	client-server
ahrs	✓	business-systems	management	1	client-server
app-powerdute	✓	business-systems	general-business	2	client-server
apple-airport	✓	networking	infrastructure	2	network-protocol
apple-update	✓	business-systems	software-update	3	client-server
argus	✓	networking	ip-protocol	1	network-protocol
ars	✓	networking	ip-protocol	1	network-protocol
asproxy	✓	networking	proxy	1	browser-based
avastar	✓	business-systems	storage-backup	2	client-server
avaya-phone-ping	✓	business-systems	management	2	client-server
avocent	✓	networking	remote-access	2	client-server
avoid	✓	networking	proxy	1	browser-based
backup-exec	✓	business-systems	storage-backup	3	client-server
badweb	✓	business-systems	erp-crm	1	browser-based
bbs-rec-recon	✓	networking	ip-protocol	1	network-protocol
belnyxc	✓	networking	remote-access	2	client-server

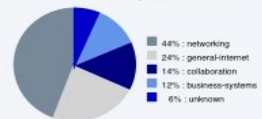
Application and Threat Summary

Apr 09, 2008

Application Usage



Category Breakdown



Top 5 Applications

Application	Sessions	Bytes
web-browsing	77,859	3,061,989,086
msrpc	46,121	5,220,877,220
icmp	38,103	5,362,784
dns	31,188	11,993,882
skype-probe	28,246	13,009,461

User Behavior

Top 5 Users

User	Sessions	Bytes
paloonetwork\binahara	743,869	53,737,432,686
paloonetwork\bsi	557,999	1,855,589,371
paloonetwork\ycheng	520,748	2,109,032,430
paloonetwork\jackson	156,793	4,230,857,356
paloonetwork\skema	131,483	6,900,749,079

Top 5 URL Categories

Category	Count
unknown	93,844
infrastructure	23,828
news	14,870
computing-and-internet	14,756
advertisements-and-popups	13,643

Top 5 Destination Countries

Destination	Count
Reserved (10.0.0.0 - 10.255.255.255)	3,267,489
United States	1,166,207
Unknown	73,266
France	70,470
China	64,917

paloonetwork\binahara

Highest Risk User

Top 5 URL Categories

Category	Count
business	13,790
unknown	10,893
computing-and-internet	3,807
infrastructure	2,784
news	1,985

Top 5 Applications

Application	Sessions	Bytes
skype-probe	957,518	485,701,118
unknown-udp	81,392	20,242,917
ssl	166,063	1,157,247,715
skype	133,752	65,618,460
msrpc	817,743	218,670,488,833

Top 5 Threats

Threat	Count
MiniBug retrieve weather information	6,890
SCAN: Host Sweep	15,956
ipwatch Mail LDAP Daemon Request Pinging Stack Overflow Vulnerability	216

Threat Types

Top 5 Spyware

Spyware	Count
MiniBug retrieve weather information	377

Top 5 Vulnerabilities

Vulnerability	Count
AWStats Remote Code Execution Vulnerability	7,336
DistCC Daemon Command Execution	5,125
Metasploit Meterpreter LSP Sanitization Remote Command Execution Vulnerability	3,558
HTTP OPTIONS Method	2,482
HTTP SQL Injection Attempt	2,372

Top 5 Viruses

Virus	Count
No matching data found!	

Threat

Top 5 Attackers

Address	Count
10.0.0.67	30,365
d9nynmc1.paloonetworks.local	21,686
binahara-xp.paloonetworks.local	15,956
binahara-pa.paloonetworks.local	12,960
pan00097.paloonetworks.local	3,888

Top 5 Victims

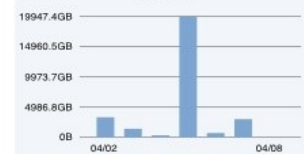
Address	Count
10.0.0.251	34,253
pa-dc-1.paloonetworks.local	8,895
pa-dc-2.paloonetworks.local	7,823
panserver.paloonetworks.local	7,226
panserver2.paloonetworks.local	6,095

Top 5 Attacker Countries

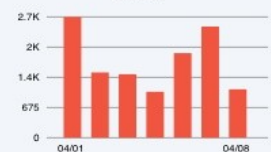
Country	Count
Reserved (10.0.0.0 - 10.255.255.255)	101,082
United States	377

Trends

Bandwidth



Threats



Opzioni Di Controllo Aggiuntive Per La Policy Di Traffic Shaping



Le policies di Traffic shaping assicurano alle applicazioni business la banda necessaria

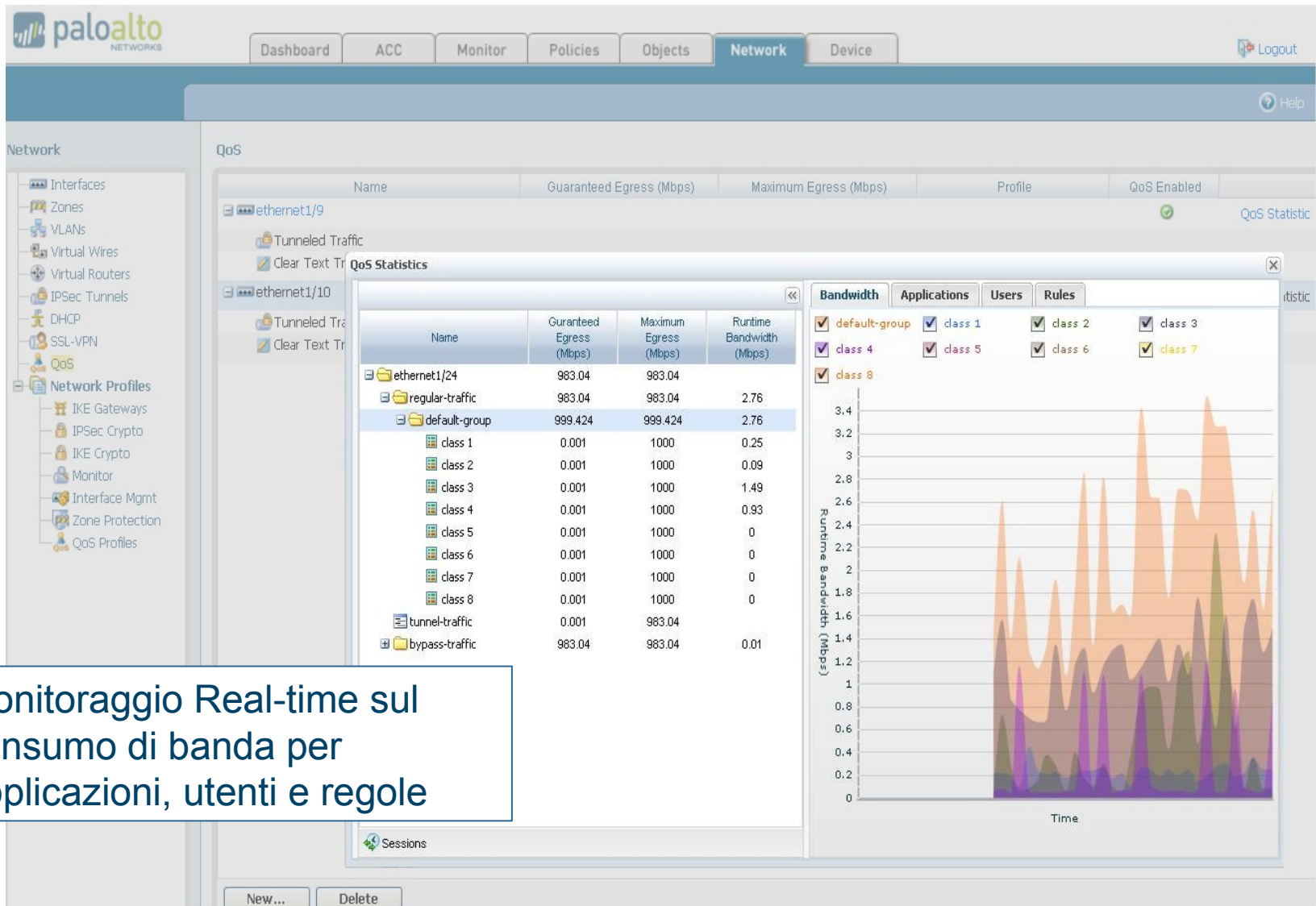
Impostazioni di larghezza di banda garantite, prioritarie e massime

Utilizzo delle policies di traffic shaping per applicazione, utente, sorgente, destinatario, interfaccia, IPSec VPN tunnel etc

Consente una maggiore efficacia nello sviluppo di adeguate politiche di utilizzo delle applicazioni

Inclusa come feature in PAN-OS senza costi aggiuntivi

Monitoraggio Real-time Della Larghezza Di Banda



Monitoraggio Real-time sul consumo di banda per applicazioni, utenti e regole

Risposta Flessibile Sul Controllo Delle Policy

Un editor intuitivo permetto un uso di policies appropriato e flessibile

• “Allow or deny” dell’utilizzo di applicazioni a livello individuale	• Consente applicando IPS, scansione di virus e spyware
• Controllo delle applicazioni per categoria, subcategoria, tecnologia o caratteristica	• Applica traffic shaping (Garantito, prioritario, massimo)
• Ispezione e decodifica SSL	• Permessi per alcuni utenti o gruppi
• Permette o/e blocca le funzioni di certe applicazioni	• Controllo utilizzo eccessivo del web surfing

paloalto NETWORKS

Dashboard ACC Monitor **Policies** Objects Network Device

Filter Rules: All Rules Source Zone: Show All Destination Zone: Show All Filter By Zone

Rulebases

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

Security Rules

	Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action	Profile	Options
1	No Intra-zone DMZ	DMZ	DMZ	any	any	any	any	any	⛔	none	
2	Do Not Traffic Log	tapzone	tapzone	any	any	LocalServers	any	any	✅	none	none
3	Do Not URL Log	tapzone	tapzone	any	any	LocalNetwork	ssl web-browsing	any	✅		
4	Monitor ALL	tapzone	tapzone	any	any	any	any	any	✅		
5	Block P2P	any	untrust	any	any	any	P2P Filesharing	any	⛔	none	
6	Webmail - No Attachments	any	untrust	any	pancademo\finance	any	Webmail	any	✅		
7	CEO YouTube	any	untrust	any	pancademo\hzielinski	any	youtube Gaming	any	✅		
8	Block High Risk Media	any	untrust	any	any	any	High Risk Media	any	⛔	none	
9	Allow IT Remote Access	trust	untrust	any	pancademo\administrators	any	Remote Access	any	✅		
10	Deny and Log Outbound	trust	untrust	any	any	any	any	any	⛔	none	
11	Deny and Log Inbound	untrust	trust	any	any	any	any	any	⛔	none	

“Identification Technologies” Trasforma il Firewall

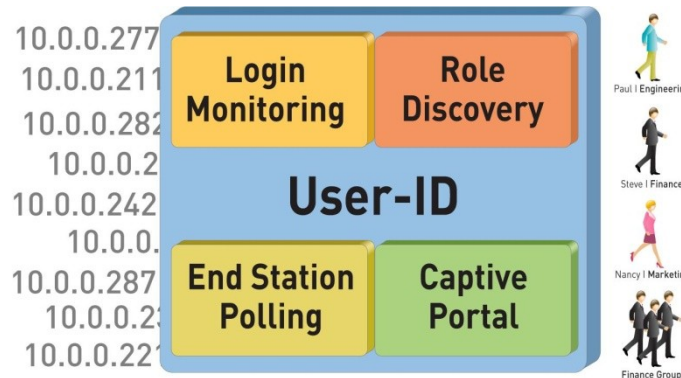
App-ID

Identifica l'Applicazione



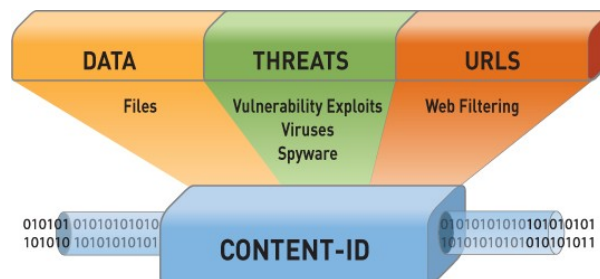
User-ID

Identifica l'Utente

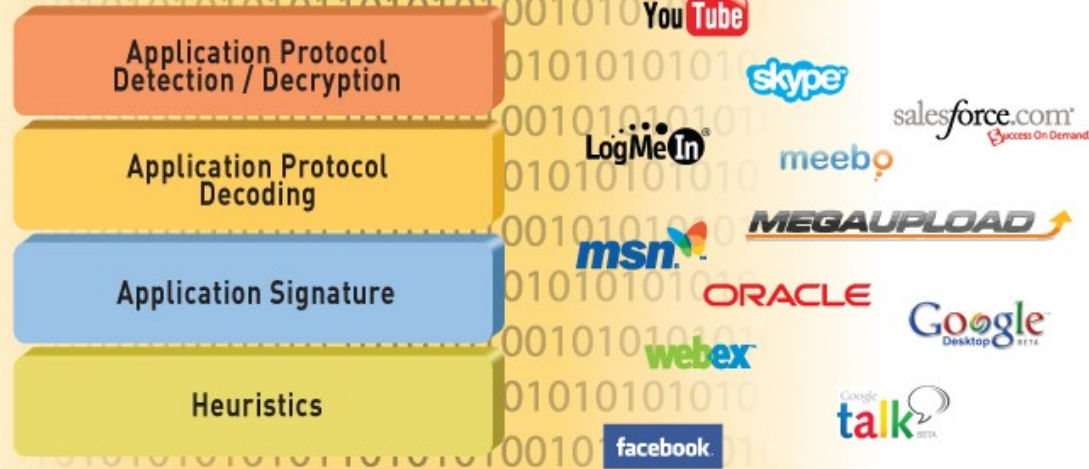


Content-ID

Scan dei contenuti

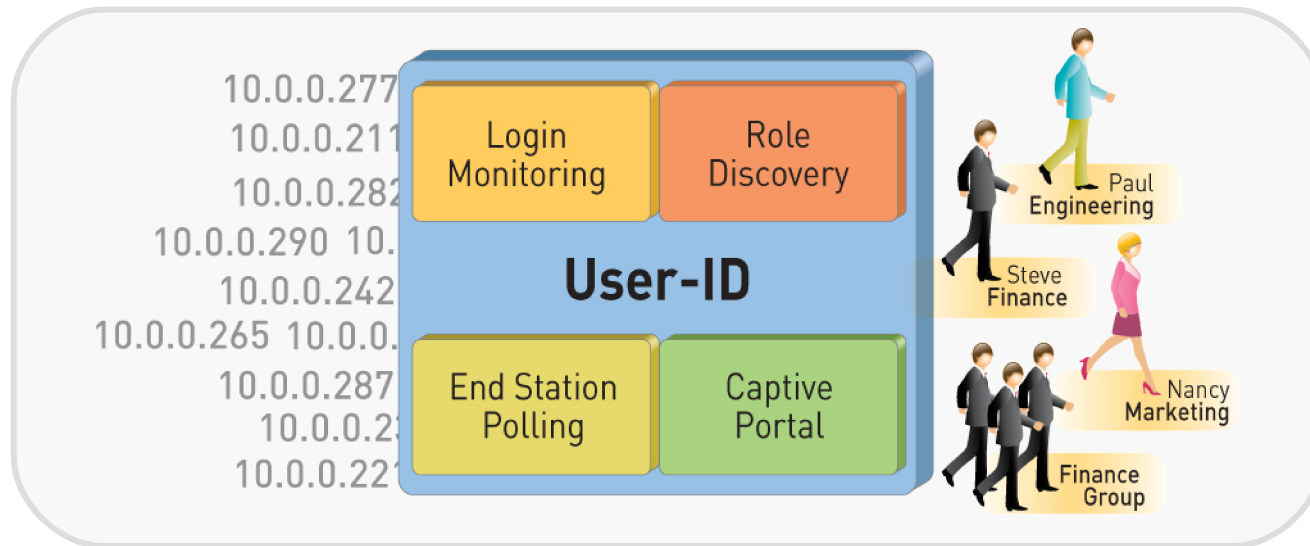


App-ID: Visibilità Globale Delle Applicazioni



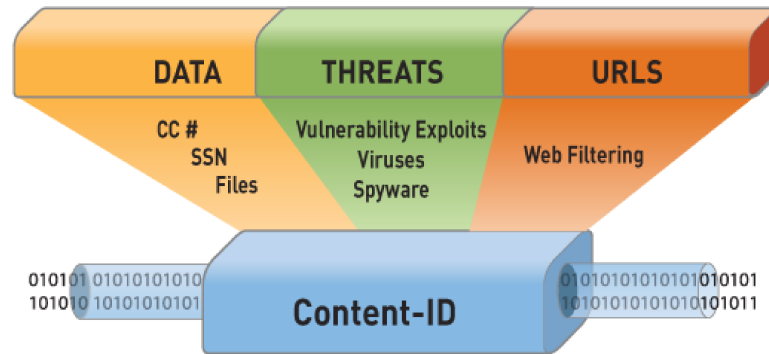
- Controllo Policie-Based su più di 1.100 applicazioni distribuite attraverso 5 categorie e 25 sub-categorie
- Mix bilanciato di business, applicazioni internet e networking e protocolli networking
- Da 3 a 5 nuove applicazioni aggiunte settimanalmente

User-ID: Integrazione Dell' Enterprise Directory



- Utenti non solo definiti da indirizzi IP
 - Utilizzo dei servizi esistenti nella directory aziendale (Active Directory, LDAP, eDirectory) senza l'installazione di agent a livello desktop
 - Identifica Utenti Citrix e politiche di relazione tra utenti e gruppi , non solo indirizzi IP
- Gestisce e rinforza le policy basate su utente e/o gruppo
- Riconosce le applicazioni utente e il comportamento della minaccia basandosi su Username, non solo IP
- Investiga sugli incidenti di Security, genera report customizzati
- Permette l'integrazione XML API con altri user repositories

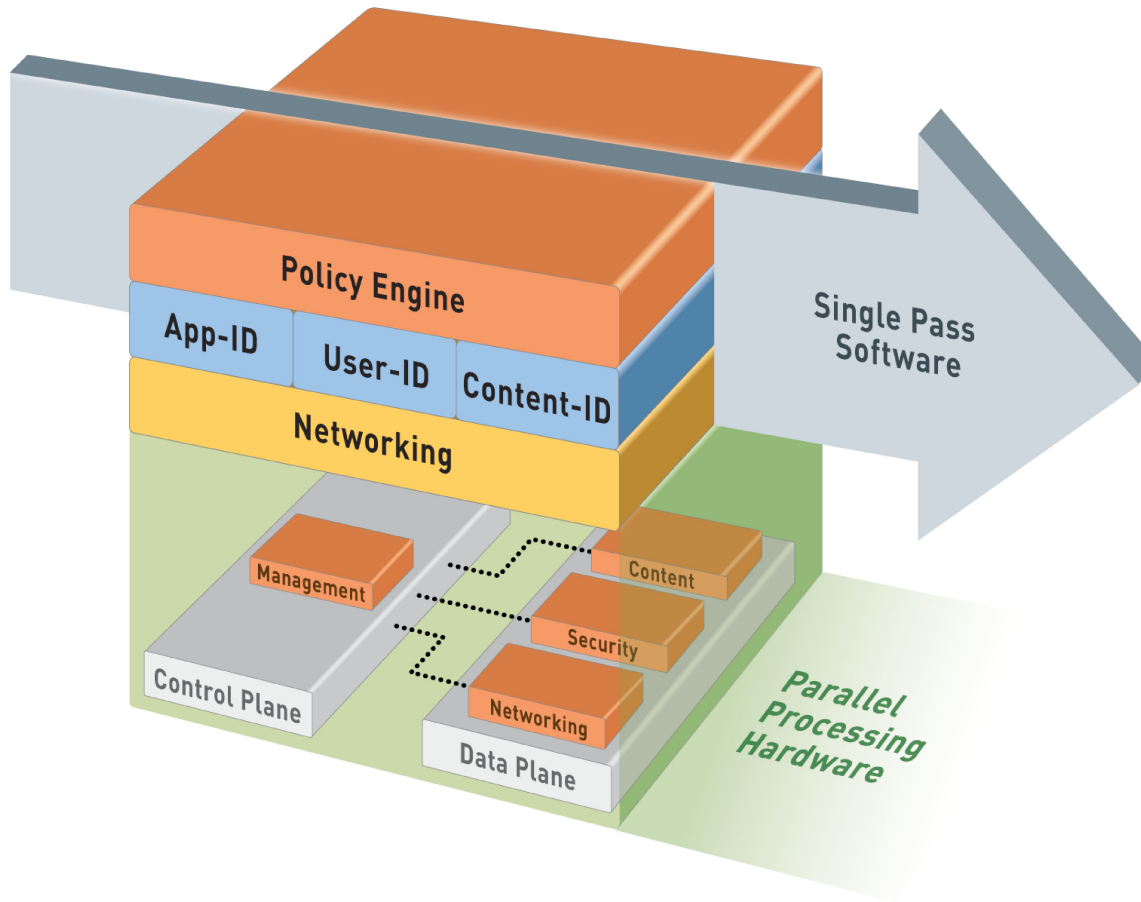
Content-ID: Real-Time Content Scanning



Individua e blocca una vasta gamma di minacce, limita il trasferimento di dati non autorizzati e controlla il web surfing non correlato al lavoro

- Stream-based, no file-based, per performance real-time
 - Scansione delle signature uniforme per una vasta gamma di minacce in un singolo passaggio
 - Vulnerability exploits (IPS), virus e spyware (sia downloads che phone-home)
- Blocca trasferimento di dati sensibili e file transfers per tipo
 - Cerca per CC # and SSN patterns
 - Cerca nel file per determinarne il tipo – non basato sulle estensioni
- Web filtering abilitato attraverso l'integrazione di un database URL
 - 20M URL (78 categorie), performance massime (1,000's URLs/sec)
 - DB dinamico e customizzabile per categorie a livello locale, regionale o industriale concentrato sul surfing patterns

Un Approccio Migliore



Architettura

Single-Pass Parallel Processing (SP3)

Single Pass

- Singolo processo per:
 - Classificazione del traffico (app identification)
 - User/group mapping
 - Content scanning – threats, URLs, DLP, etc.

- Una policy

Parallel Processing

- Function-specific hardware engines
- Multi-core security processing
- Data/control planes separati

Fino a 10Gbps, Bassa Latenza

Trace Session Tool

Refresh Manual Rows 20 Resolve

Threat Log

Filter:

	Receive Time	Type	Name	ID
	02/02 16:47:36	vulnerability	FTP: login brute force attempt	40001
	02/02 16:46:58	virus	Virus/Win32.Libis.a	20138
	02/02 16:46:40	vulnerability	FTP: login brute force attempt	40001
	02/02 16:46:12	spyware	MyWebSearch_Toolbar startup configuration	10704
	02/02 16:46:02	virus	Virus/Win32.Libis.a	20138
	02/02 16:45:49	vulnerability	FTP: login brute force attempt	40001
	02/02 16:45:40	vulnerability	HTTP OPTIONS Method	30520
	02/02 16:45:03	virus	Trojan/Js.Iframe.bs	25442
	02/02 16:44:27	vulnerability	FTP: login brute force attempt	40001
	02/02 16:44:15	vulnerability	NetBIOS nbstat query	31707
	02/02 16:43:45	vulnerability	FTP: login brute force attempt	40001
	02/02 16:42:55	vulnerability	FTP: login brute force attempt	40001
	02/02 16:42:17	vulnerability	HTTP OPTIONS Method	30520
	02/02 16:41:41	vulnerability	HTTP OPTIONS Method	30520
	02/02 16:41:27	vulnerability	HTTP OPTIONS Method	30520
	02/02 16:41:20	vulnerability	FTP: login brute force attempt	40001
	02/02 16:41:13	vulnerability	Microsoft IIS Sample Scripts Arbitrary File Disclosure Vulnerability	30323
	02/02 16:40:09	vulnerability	FTP: login brute force attempt	40001
	02/02 16:39:09	vulnerability	FTP: login brute force attempt	40001
	02/02 16:38:39	software	WinHlp 10.0.368 Get Image Request	11964

Page: 1 2 3 4 5 6 7 8 9 10

Log	THREAT
Type	vulnerability
Receive Time	2010/02/02 16:41:13
Generation Time	2010/02/02 16:41:09
Threat Name	Microsoft IIS Sample Scripts Arbitrary File Disclosure Vulnerability
Threat ID	30323
Direction	client-to-server
From Zone	untrust
To Zone	untrust
Attacker	10.154.12.189
Victim	216.128.29.26
From User	pancademo\vivian.brown
To User	
From Port	3911
To Port	80
Protocol	tcp
Application	web-browsing
Action	alert
Severity	medium
Rule	Monitor ALL
Ingress I/F	ethernet1/1
Egress I/F	ethernet1/2
Log Action	toBetaRama
Virtual System	vsys1
Session Id	684617
Count	1
Configuration Version	3
Category	any
Others	
SSL Decrypted	no
NAT Applied	no
Packet Capture	yes
Captive Portal	no
Proxy Transaction	no
Serial #	0001A100211

	Receive Time	Log	Type	Application	Action	Rule	Details
	02/02 16:41:08	THREAT	url	web-browsing	alert	Monitor ALL	Severity: informational Category: training-and-tools URL: w3schools.com/asp/showcode.asp?source=demo_array
	02/02 16:41:13	THREAT	vulnerability	web-browsing	alert	Monitor ALL	Severity: medium ID: 30323 Name: Microsoft IIS Sample Scripts Arbitrary File Disclosure Vulnerability
	02/02 16:42:43	TRAFFIC	end	web-browsing	allow	Monitor ALL	Bytes: 2156 Packets: 7

Migliora le indagini sia per incidente che a livello forense – Visualizza tutti I logs da altri databases su particolari sessioni.

From Port	To Port	Application	Action	Severity
30782	21	ftp	alert	medium
30	1072	web-browsing	alert	medium
38267	21	ftp	alert	medium
30	49473	web-browsing	alert	medium
30	1053	web-browsing	alert	medium
35929	21	ftp	alert	medium
2617	80	web-browsing	alert	informational
30	58752	web-browsing	alert	medium
42409	21	ftp	alert	medium
137	137	netbios-ns	alert	low
16544	21	ftp	alert	medium
16714	21	ftp	alert	medium
31344	80	web-browsing	alert	informational
11024	80	blackboard	alert	informational
38071	80	blackboard	alert	informational
32181	21	ftp	alert	medium
3911	80	web-browsing	alert	medium
38923	21	ftp	alert	medium
17051	21	ftp	alert	medium
30	2430	web-browsing	alert	medium