A Comprehensive CyberSecurity Policy

Review of ALL NGFW Capabilities

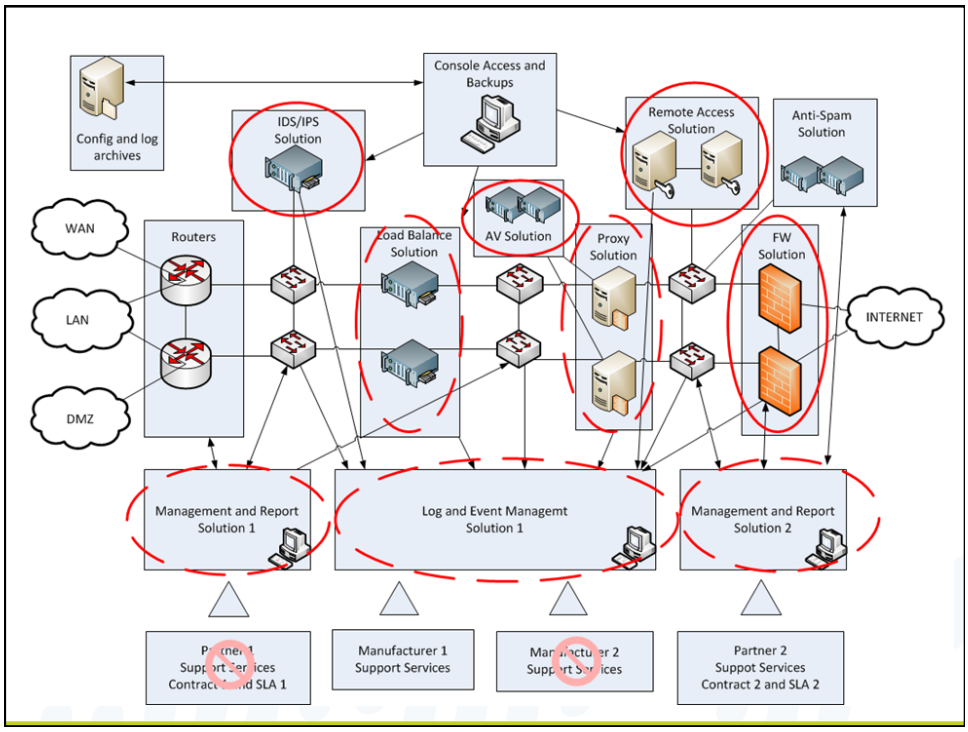
Attack Surface Reduction

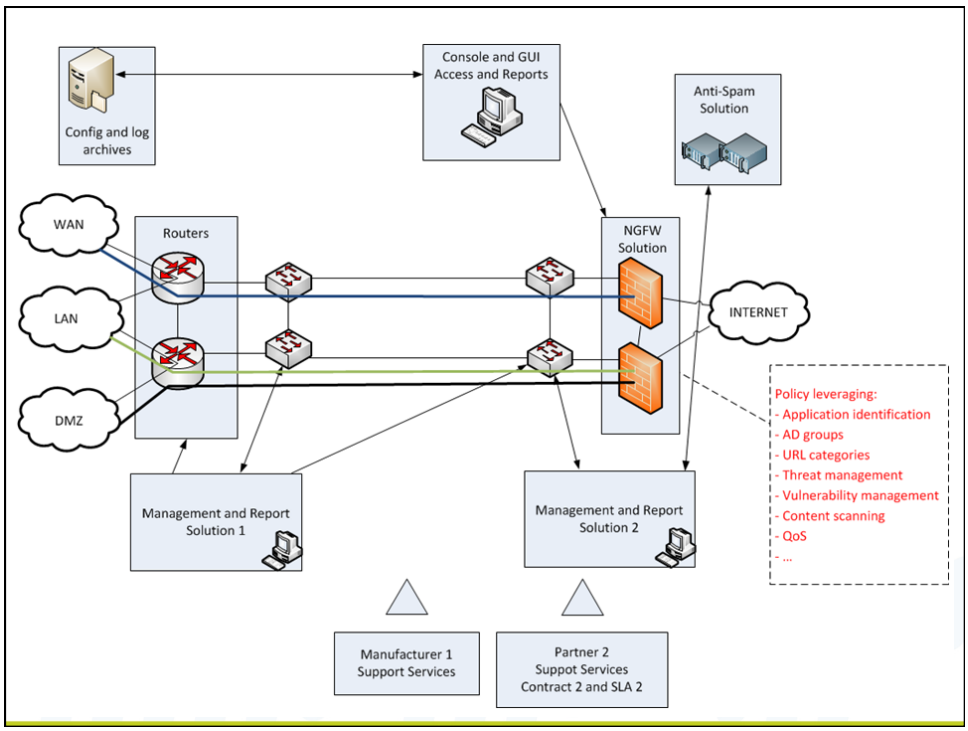
paloalto NETWORKS
the network security company™

From Complex to Comprehensive

Before and After of a PANW customer

paloalto NETWORKS
the network security company™


Config and log archives
Console Access and Backups
IDS/IPS Solution
Remote Access Solution
Anti-Spam Solution
WAN
Routers
Load Balance Solution
AV Solution
Proxy Solution
FW Solution
LAN
INTERNET
DMZ
Management and Report Solution 1
Log and Event Managemt Solution 1
Management and Report Solution 2
Manufacturer 1 Support Services
Partner 2 Suppot Services Contract 2 and SLA 2


Config and log archives
Console and GUI Access and Reports
Anti-Spam Solution
WAN
Routers
NGFW Solution
LAN
INTERNET
DMZ
Policy leveraging:
- Application identification
- AD groups
- URL categories
- Threat management
- Vulnerability management
- Content scanning
- QoS
- ...
Management and Report Solution 1
Management and Report Solution 2
Manufacturer 1 Support Services
Partner 2 Suppot Services Contract 2 and SLA 2

1 Enhanced Policy on the L7 layer

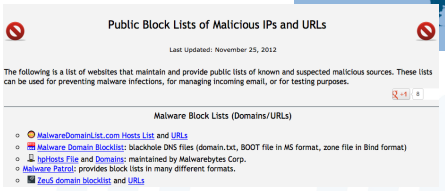
paloalto NETWORKS
the network security company™

Leverage ALL NGFW Capabilities - Location

- Limit Sources and Destinations of traffic
  - Restricted IP Ranges
  - Countries
  - Specific known bad IP's
  - Dynamic Block Lists
  - Known Users/Groups

DNS-BH – Malware Domain Blocklist

Malware Prevention through Domain Blocking (Black Hole DNS Sinkhole)



Public Block Lists of Malicious IPs and URLs

Last Updated: November 25, 2012

The following is a list of websites that maintain and provide public lists of known and suspected malicious sources. These lists can be used for preventing malware infections, for managing incoming email, or for testing purposes.

Malware Block Lists (Domains/URLs)

- MalwareDomainList.com Hosts List and URLs
- Malware Domain Blocklist: blackhole DNS files (domain.txt, BOOT file in MS format, zone file in Bind format)
- hpHosts File and Domains: maintained by Malwarebytes Corp.
- Malware Patrol: provides block lists in many different formats.
- ZeuS domain blocklist and URLs

Slide 6

paloalto NETWORKS

Leverage ALL NGFW Capabilities - Applications

- Limit Sources and Destinations of traffic
  - Restricted IP Ranges / Countries
  - Known Users/Groups
  - Specific known bad IP's / Dynamic Block Lists
- Control Application Usage (Positive Enforcement / Default Deny)
  - Avoid High risk -- File Transfer and Tunneling Applications
  - Reduce or avoid the need for unknown-udp/tcp usage
  - Allow legitimate applications

FTP was a surprisingly evasive and effective malware vector
- 95% of malware delivered via FTP were never detected by traditional AV (in a 30 day period).
- 97% of malware sessions used non-standard ports..

2013 Modern Malware Review

Webmail is a very common delivery vector for Malware
- Yahoo-Mail, AIM-Mail, Hotmail, Mail.ru are among the top 15 apps that deliver malware

- SMTP, POP3, and other common mail apps make the list as well

2013 Modern Malware Review

Slide 7

paloalto NETWORKS

Leverage ALL NGFW Capabilities - Applications

- Limit Sources and Destinations of traffic
  - Restricted IP Ranges / Countries
  - Known Users/Groups
  - Specific known bad IP's / Dynamic Block Lists
- Control Application Usage (Positive Enforcement / Default Deny)
  - Avoid High risk -- File Transfer and Tunneling Applications
  - Reduce or avoid the need for unknown-udp/tcp usage
  - Allow legitimate applications

4	ms-exchange	collaboration	email	client-server	90,489,681,905
5	smtp	collaboration	email	client-server	52,324,415,049
4	gmail-base	collaboration	email	browser-based	19,770,419,222
4	hotmail	collaboration	email	browser-based	6,866,089,186
4	lotus-notes-base	collaboration	email	client-server	3,790,633,781
4	aim-mail	collaboration	email	browser-based	2,491,264,136
4	daum-mail	collaboration	email	browser-based	489,740,012
5	horde	collaboration	email	browser-based	169,785,104
4	netease-mail	collaboration	email	browser-based	153,522,284
4	squirrelmail	collaboration	email	browser-based	151,349,028
4	qq-mail	collaboration	email	browser-based	25,783,996
4	gmail-enterprise	collaboration	email	browser-based	7,152,024
4	outlook-web	collaboration	email	browser-based	4,528,330
4	mail.ru-mail	collaboration	email	browser-based	2,024,370
4	yandex-mail	collaboration	email	browser-based	1,846,624
4	blackberry	collaboration	email	client-server	1,286,040
4	imap	collaboration	email	client-server	1,190,047
4	roundcube	collaboration	email	browser-based	1,134,478
4	telenet-webmail	collaboration	email	browser-based	509,056
4	gmx-mail	collaboration	email	browser-based	489,832
4	pop3	collaboration	email	client-server	58,248
4	web-de-mail	collaboration	email	browser-based	44,616

22 Email Apps

4	dropbox	general-internet	file-sharing	client-server	71,306,108,068
4	sharefile	general-internet	file-sharing	browser-based	28,965,723,195
4	skydrive-base	general-internet	file-sharing	browser-based	12,051,827,913
4	yousendit-base	general-internet	file-sharing	browser-based	3,169,186,574
5	ftp	general-internet	file-sharing	client-server	2,972,890,312
5	webdav	general-internet	file-sharing	browser-based	2,374,813,805
4	rapidshare	general-internet	file-sharing	browser-based	2,229,394,510
4	4shared	general-internet	file-sharing	browser-based	895,149,103
5	dl-free	general-internet	file-sharing	browser-based	314,531,348
4	sendspace	general-internet	file-sharing	browser-based	196,068,719
4	google-drive	general-internet	file-sharing	browser-based	79,280,129
5	bittorrent	general-internet	file-sharing	peer-to-peer	41,849,043
4	docstoc-base	general-internet	file-sharing	browser-based	107,144,990
4	live-mesh-base	general-internet	file-sharing	client-server	64,812,019
4	mediafire	general-internet	file-sharing	browser-based	27,960,135
5	xunlei	general-internet	file-sharing	peer-to-peer	9,447,431
4	tftp	general-internet	file-sharing	client-server	6,378,966
4	leapfile	general-internet	file-sharing	browser-based	1,866,442
4	office-live	general-internet	file-sharing	client-server	1,764,052
5	fileserve	general-internet	file-sharing	browser-based	1,758,672
4	putlocker	general-internet	file-sharing	browser-based	911,649
4	divshare	general-internet	file-sharing	browser-based	806,216

34 File Sharing Apps

Slide 8

paloalto NETWORKS

Leverage ALL NGFW Capabilities - Browsing

- Limit Sources and Destinations of traffic
  - Restricted IP Ranges / Countries
  - Known Users/Groups
  - Specific known bad IP's / Dynamic Block Lists
- Control Application Usage (Positive Enforcement / Default Deny)
  - Avoid High risk -- File Transfer and Tunneling Applications
  - Reduce or avoid the need for unknown-udp/tcp usage
  - Allow legitimate applications
- Limit Web browsing activity
  - Malware
  - Adult & Pornography
  - Unknown

- 94% of unknown malware was delivered via web-browsing or web proxies.
- It took traditional antivirus 4x as long to provide coverage for malware delivered from the web as opposed to email (20 days for web vs 5 days for email).

URL Category	Action
adult	decrypt
malware	
not-resolved	
nudity	
unknown	
financial-services	no-decrypt
health-and-medi...	

Slide 9

paloalto NETWORKS

Leverage ALL NGFW Capabilities – Known Threats

- Limit Sources and Destinations of traffic
  - Restricted IP Ranges / Countries
  - Known Users/Groups
  - Specific known bad IP's / Dynamic Block Lists
- Control Application Usage (Positive Enforcement / Default Deny)
  - Avoid High risk -- File Transfer and Tunneling Applications
  - Reduce or avoid the need for unknown-udp/tcp usage
  - Allow legitimate applications
- Limit Web browsing activity
  - Malware
  - Adult & Pornography
  - Unknown
- Scan for Threats within allowed traffic
  - Exploits
  - Malware / Spyware
  - Virus

Slide 10

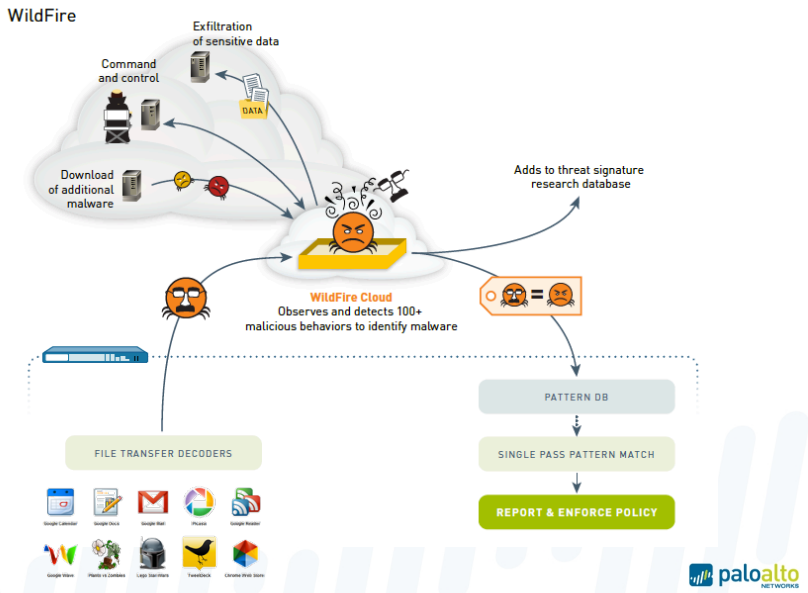
paloalto NETWORKS

- Limit Sources and Destinations of traffic
  - Restricted IP Ranges / Countries
  - Known Users/Groups
  - Specific known bad IP's / Dynamic Block Lists
- Control Application Usage (Positive Enforcement / Default Deny)
  - Avoid High risk -- File Transfer and Tunneling Applications
  - Reduce or avoid the need for unknown-udp/tcp usage
  - Allow legitimate applications
- Limit Web browsing activity
  - Malware
  - Adult & Pornography
  - Unknown
- Scan for Threats within allowed traffic
  - Exploits
  - Malware / Spyware
  - Virus

User Identification

Single Policy

ONLY THEN… Bring in the Sandbox!



Slide 12

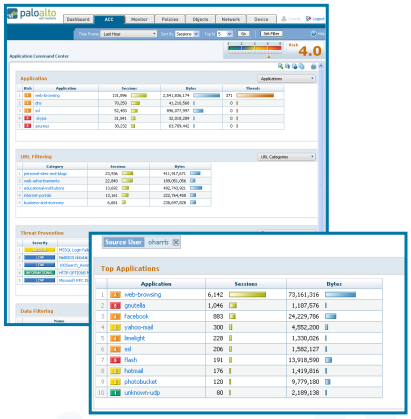
paloalto NETWORKS

Policy Example…

paloalto NETWORKS
the network security company™

Policy Development Intelligence & Background

- First understand your network and use visibility tools from Palo Alto Networks' NGFW
  - Application Usage
  - Source / Destination Information
  - Threat Activity
  - User Behavior
  - Web Browsing behavior
- Use WildFire to track
  - How Malware got in using/via which
    - Applications, Websites, Countries, Users
- Review the enterprises business requirements
  - Partner Communication requirements
  - Necessary Applications
  - Internet Usage Policy
- Set your Policy Goals:
  - Do not hinder computing and communication needs of the users
  - Protect the Organization from Malware

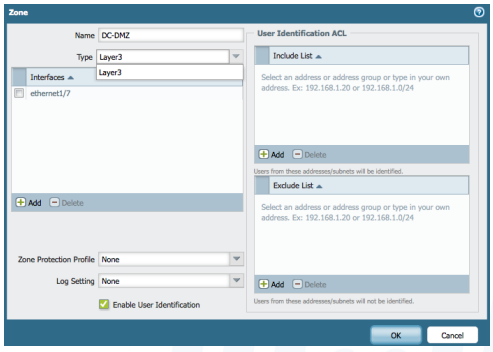


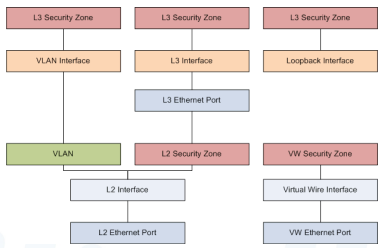
Some definitions…

paloalto NETWORKS
the network security company™

ZONES… -- Important for Network Segmentation

- Logical Containers for physical interfaces, VLANs, IP Ranges
- All interfaces must be part of a zone
- Purpose of the NGFW is to control traffic between Zones
- Policy execution focuses on just relevant Zone – Zone traffic



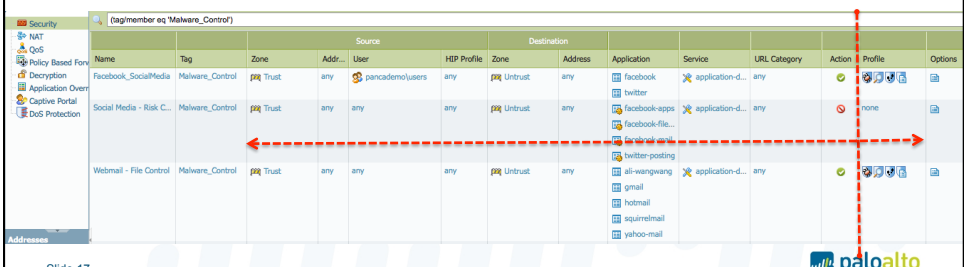


Slide 16

paloalto NETWORKS

Policy Elements

- Security Policy fundamentally controls traffic between **Zones**
- Leverage many more criteria (“tuples”) than in a traditional Firewall
- Common Elements - SRC_Addr, DST_Addr, SRC_Port, DST_Port
- **PLUS:** Zone, User/Group, HIP Profile, Application, URL Category
- Single Policy with security controls and content inspection → Security Profiles
- Rule options – Log forwarding, Scheduling, etc…
- Tags – allow for logical grouping and management

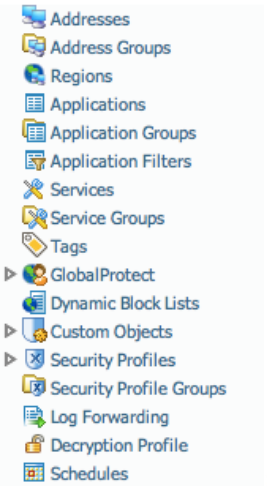


Slide 17

paloalto NETWORKS

Objects

- Policy Elements that can be pre-defined and reused in the construction of Policies.
- Modification of the object (vs the policy itself) allows the policy framework to remain fixed while the objects change.
- Types of Objects
  - Applications
  - Addresses / Regions
  - Dynamic Block Lists
  - Custom Categories
  - Custom Signatures
  - Service Objects
  - Security Profiles
  - Log Forwarding
  - Schedules

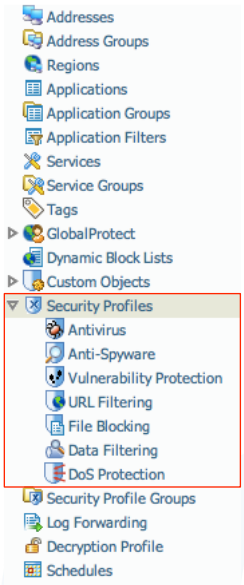


Slide 18

paloalto NETWORKS

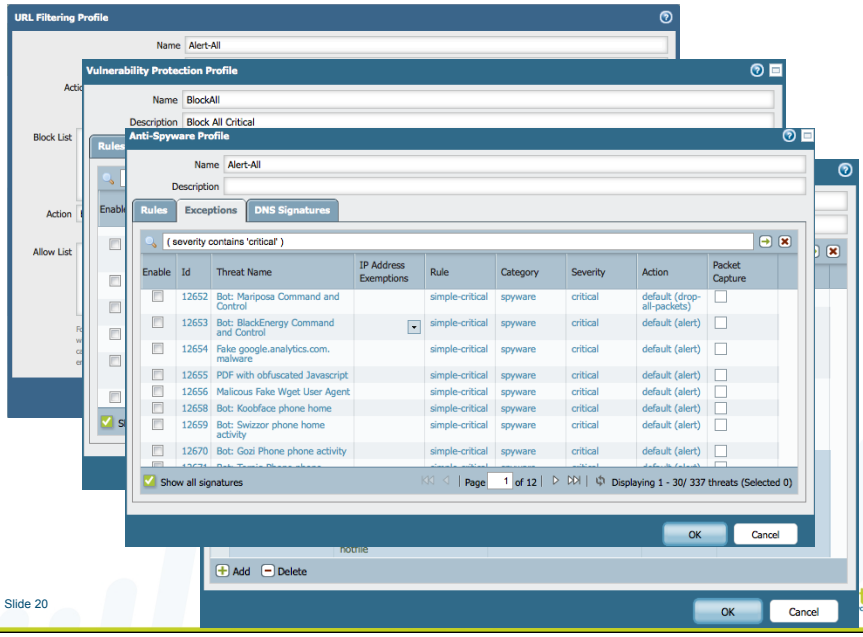
Security Profiles = Objects used in Policies/Rules

- Profiles are defined as objects and used granularly throughout the entire Policy
- Used in combination with other profiles
  - IPS, Anti-Virus, Spyware, File Control, etc...
- Targeted at Specific Users, Zones, Address Groups, Regions -- Rules
- Variety of Actions available – Block/ Continue/… independent of Firewall Allow / Deny



Slide 19

Profiles



Slide 20

The Policy Visualized

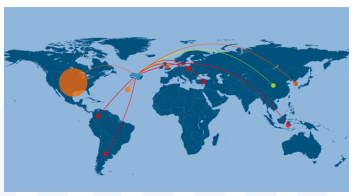
paloalto NETWORKS
the network security company™

Control the sources of traffic

- Inbound Control
  - Block traffic From Countries you do no Business with
- Use Geo or Region Objects; combined with the “Deny” action for all traffic
  - Consider the “Negate” feature on the Source Objects

		Source				Destination						
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile
Deny Geo Inbound	Malware_Control	Untrust	AU CA CH GB US	any	any	DMZ Trust Untrust	any	any	any	any		none

- Eliminates a broad swath of unnecessary traffic
- Utilize Source Country Address filters
- The “Negate” feature combined with the “Deny” action
- Targeted Between Zones
  - Untrust -> DMZ
  - Untrust -> Untrust
  - Untrust -> Trust
- Logging Enabled on rule



Slide 22

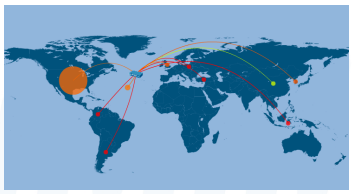
paloalto NETWORKS

Control Outbound Destinations (User Traffic)

- Outbound Control
  - Block SSL and Web traffic To Countries you do no Business with
- Consider the “Negate” feature; select applications; and the “Deny” action

		Source				Destination						
Name	Tag	Zone	Addr...	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile	Options
Deny Geo Outbound	Malware_Control	Trust	any	any	any	Untrust	AU CA GB IL US	ssl web-browsing	application-d...	any		none	

- Controls Outbound user traffic to unnecessary destinations
- Utilize Destination Country Address filters
- Targeted Between Zones
  - Trust -> Untrust
- Leverages App-ID
  - SSL & Web Browsing
  - On their Default Ports
- Logging Enabled on rule



Slide 23

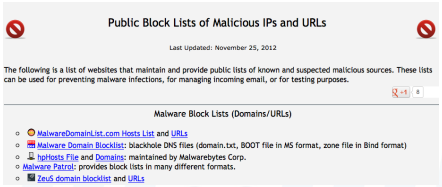
paloalto NETWORKS

Eliminate Traffic from known Malicious sources

- Block Known Malicious Sources
- Custom or Dynamic Block List source address; combined with the “Deny” action

		Source				Destination						
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile
External Block - Known	Malware_Control	Untrust	BadRussianHac...	any	any	DMZ Trust Untrust	any	any	any	any		none

- Leverage existing list of known sources of attack
- Targeted Between Zones
  - Untrust -> DMZ
  - Untrust -> Untrust
  - Untrust -> Trust
- Logging Enabled on rule



Slide 24

paloalto NETWORKS

Control Legacy File Transfer Applications

- Leverage User Groups identifying IT and/or Authorized Users
- Zone and User Group(s) as sources; well defined applications; “Allow” action
- Inspect allowed traffic

		Source				Destination							
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile	Options
File Transfer - Per User	Malware_Cont...	Trust	any	pancademo\admini... pancademo\domai... pancademo\networ... pancademo\qa - a... pancademo\sharep... pancademo\user - ...	any	Untrust	any	ftp ssh tftp	application-d...	any			

- Regulate how approved File Transfer applications are used
- Limit what users can leverage File Transfers outbound
- Ensure that FTP (and SSH) are only used on their default ports
- Inspect allowed traffic with IPS, AntiVirus, File Blocking, and other content controls.
- Targeted Between Zones
  - Trust -> Untrust
- Logging Enabled on rule

FTP was a surprisingly evasive and effective malware vector
- 95% of malware delivered via FTP were never detected by traditional AV (in a 30 day period).
- 97% of malware sessions used non-standard ports..

2013 Modern Malware Review

Slide 25

Safely Allow SOME social networking and behavior

- Zone and User Group(s) as sources; well defined applications; “Allow” action
- Inspect allowed traffic
- Block unwanted sub-applications

		Source				Destination						
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile
Facebook_SocialMedia	Malware_Control	Trust	any	pancademo\users	any	Untrust	any	facebook twitter	application-d...	any		
Social Media - Risk C...	Malware_Control	Trust	any	any	any	Untrust	any	facebook-apps facebook-file... facebook-mail twitter-posting	application-d...	any		none

- Manage the use of social networking applications and their functions
- Ensure that Social Networking only runs on its default port
- Inspect allowed traffic with IPS, AntiVirus, File Blocking, and other content controls.
- DENY the “Facebook Apps” and other sub function for all users.
  - Most common social networking threat and malware vector
- Targeted Between Zones
  - Trust -> Untrust
- Logging Enabled on rule

Facebook-Apps accounts for 97% of all threats within social networking traffic.

2013 Application usage and Threat report

Slide 26

Control Webmail file attachments

- Review and allow select webmail applications or use applications filters
- Prevent downloads of exe/PE/Bat/jar files for all or most users

		Source				Destination						
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile
Webmail - File Control	Malware_Control	Trust	any	any	any	Untrust	any	ali-wangwang gmail hotmail squirrelmail yahoo-mail	application-d...	any		

- Allow the use of Webmail & Collaboration application cetegories, but…
- Deny the ability to move certain file types with these applications
- Inspect allowed traffic with IPS, AntiVirus, File Blocking, and other content controls.
- Targeted Between Zones
  - Trust -> Untrust
- Logging Enabled on rule

Webmail is a very common delivery vector for Malware
- Yahoo-Mail, AIM-Mail, Hotmail, Mail.ru are among the top 15 apps that deliver malware
- SMTP, POP3, and other common mail apps make the list as well
2013 Modern Malware Review

Control File Movement – File Blocking Profile

- Define 1 or more File Blocking Profiles
- Use them selectively in the correct rules ≠ 1 firewall wide file blocking policy

File Blocking Profile

Name: Webmail_File_Policy
Description: File types that are allowed for download and upload for both Webmail and Websites

Names	Applications	File Types	Direction	Action
Webmail DnLd Block	any	PE bat exe jar torrent	download	block
Webmail Log	any	any	both	alert

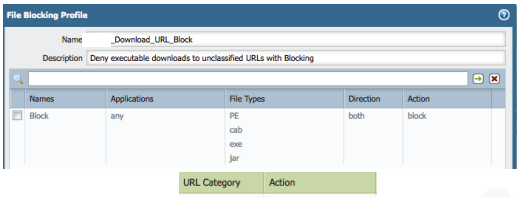
- File Blocking “Object” is targeted at a specific rule allowing specific traffic.
- “Policy within a Policy”
- Criteria: Application, File Type, Direction, Action

Control User File download behavior

- Use the File Blocking and Security Profiles leveraging multiple 'match' criteria
  - Zone, User or Group, Application(s) and URL categories

		Source				Destination						
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile
Unknown URL Protec...	Malware_Control	Trust	any	pancademo\finance pancademo\market... pancademo\mobile... pancademo\user - i... pancademo\users	any	Untrust	any	web-browsing	any	adult unknown		

- Targets specific users and their web browsing behavior
- Prevents certain high risk file types from being delivered by visiting certain web sites.
- Inspects all allowed traffic with IPS, AV, Spyware, Malware
- Combined with SSL Decryption this can stop a common infection vector

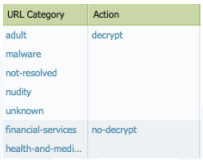


File Blocking Profile

Name: _Download_URL_Block

Description: Deny executable downloads to unclassified URLs with Blocking

Names	Applications	File Types	Direction	Action
Block	any	PE cab exe jar	both	block



URL Category	Action
adult	decrypt
malware	
not-resolved	
nudity	
unknown	
financial-services	no-decrypt
health-and-medi...	

URL Filtering Profile

- Define correct URL Filtering Profiles
- If required, use custom URL Categories or populate Block/Allow Lists

Name	Location	Action on License Expiration	Block List	Action for Block List	Allow List	Allow Categories *	Alert Categories	Block Categories
Content_ID		allow	*.myspace.com *.plaxo.com *.newsoftspot... *.newsoftspot... *.babylon.com *.clubbing.com www.arcadew... more...	block	www.centralse... www.centralse.../timeout.asp www.centralse... 63.241.139.139 www.nhlottery... www.nhlottery... 65.55.177.205 more...	CH_URLS_Not-to-Log *	CH-PANDB-Wrong-Class * abortion abused-drugs alcohol-and-tobacco auctions business-and-economy computer-and-internet-info more...	CH-Untrusted-Sites * adult-and-pornography bot-nets cheating confirmed-spam-sources dating games more...

- Utilize Categorical selections to block access to unwanted or prohibited web destinations
- Logging enabled for allowed and blocked sites
- User information captured for all browsing activity.

Control Web Browsing Behavior

- Use URL and Content Filtering Profiles to control Internet access
- Use correct Zone, User or Group, Application(s) objects

		Source				Destination					
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile
General Web	inbound	trust	any	pansgdemo\f... pansgdemo\g...	any	untrust	any	web-browsing ssl	any		

- Targets specific users and their web browsing behavior
- Prevents certain high risk file types from being delivered by visiting certain web sites.
- Inspects all allowed traffic with IPS, AV, Spyware, Malware
- Combined with SSL Decryption this can stop a common infection vector

File Blocking Profile

Name: _Download_URL_Block

Description: Deny executable downloads to unclassified URLs with Blocking

Names	Applications	File Types	Direction	Action
Block	any	PE cab exe jar	both	block

URL Category	Action
adult	decrypt
malware	
not-resolved	
nudity	
unknown	
financial-services	no-decrypt
health-and-medi...	

paloalto NETWORKS

Control high risk / prohibited applications

- In case some flexible Internet Application use is allowed; reduce the risk
- Block high risk application categories, using Application Filters

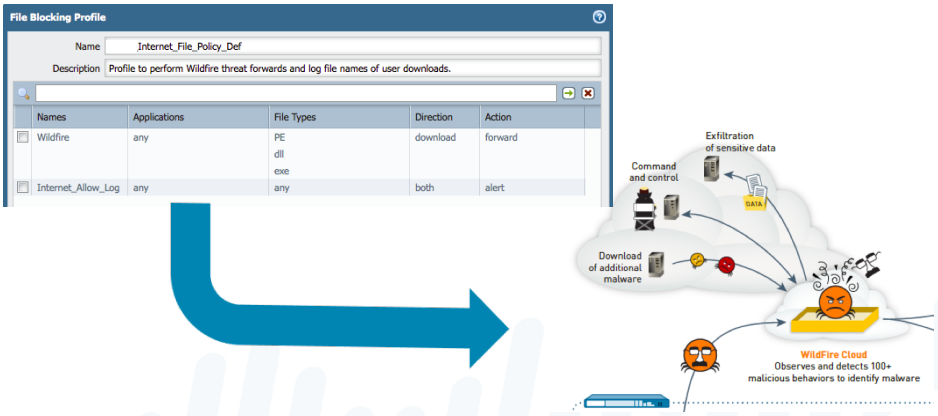
		Source				Destination					
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile
High Risk Applications	Malware_Control	Trust	any	any	any	Untrust	any	Gaming Proxies bittorrent hamachi tor ultrasurf	application-d...	any		none

- Deny the use of applications that are prohibited by internet usage policy
- Targeted Between Zones
  - Trust -> Untrust
- Logging Enabled on rule

paloalto NETWORKS

If a file passes the previous controls – WILDFIRE!

- Use a WildFire enabled File Blocking Profile when File Downloads are allowed
- Review logs and keep on tuning your policy
- Benefit from the WildFire research; enhancing all layers of Threat Prevention



Slide 33

paloalto NETWORKS

The Results of Wildfire

- Expanding the KNOWN threats – near real time
  - New **Unique** Malware Signatures – in less than 1 hour
  - DNS Signatures – DNS lookups for host names associated with Malware
  - Malware URL's – Constantly added to the URL Filtering Database
  - Command & Control (C&C) signatures – added to the Spyware database
- Important Security Intelligence – to help refine policy
  - High Risk Applications – which applications communicate Malware?
  - High Risk Users – Which users have behavior that exposes them?
  - Sources of Malware – IP Addresses, URL's, Geographic Regions
  - Destinations of Malware – where do infected hosts communicate to?

Slide 34

paloalto NETWORKS


paloalto
NETWORKS
the network security company™