Introducing PAN-OS and Panorama 7.0

June 2015

paloalto NETWORKS

the network security company™

Contents

- Highlighted features
  - Management/Panorama
  - WildFire
  - App-ID/User-ID
  - Virtualization
  - Decryption
  - Hardware
- Summary of all other features
- Detail on the rest of the features

Millions of events — which are important?

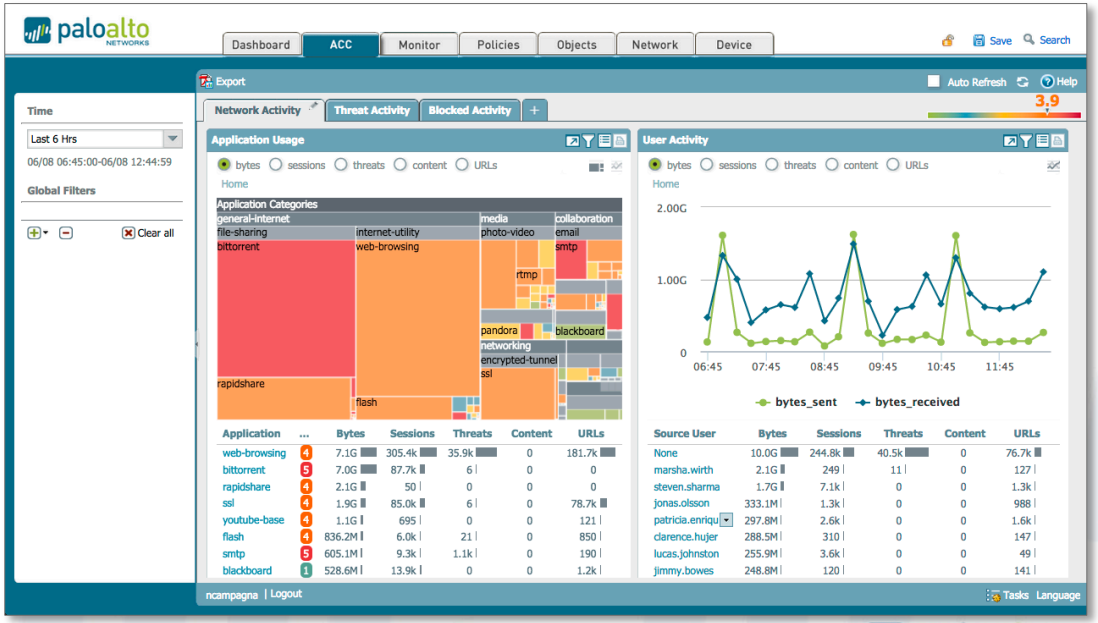
Context is critical

- Identify visually through redesigned ACC
  - Leverage all types of events within ACC
  - View events over time to identify anomalies or patterns
  - Quickly pivot on any element to get further detail or a different view
- Identify through correlation with new Automated Correlation Engine
  - Identify malicious activity that would not otherwise stand out
  - Focus effort on confirmed issues rather than partial information

Redesigned ACC

- Create a ***starting point*** for answering important network security questions
- Provide prioritized, ***actionable*** information with minimal data mining
- Leverage ***all*** of our data

- Clean
- Comprehensive
- Historical
- Customizable



Redesigned ACC

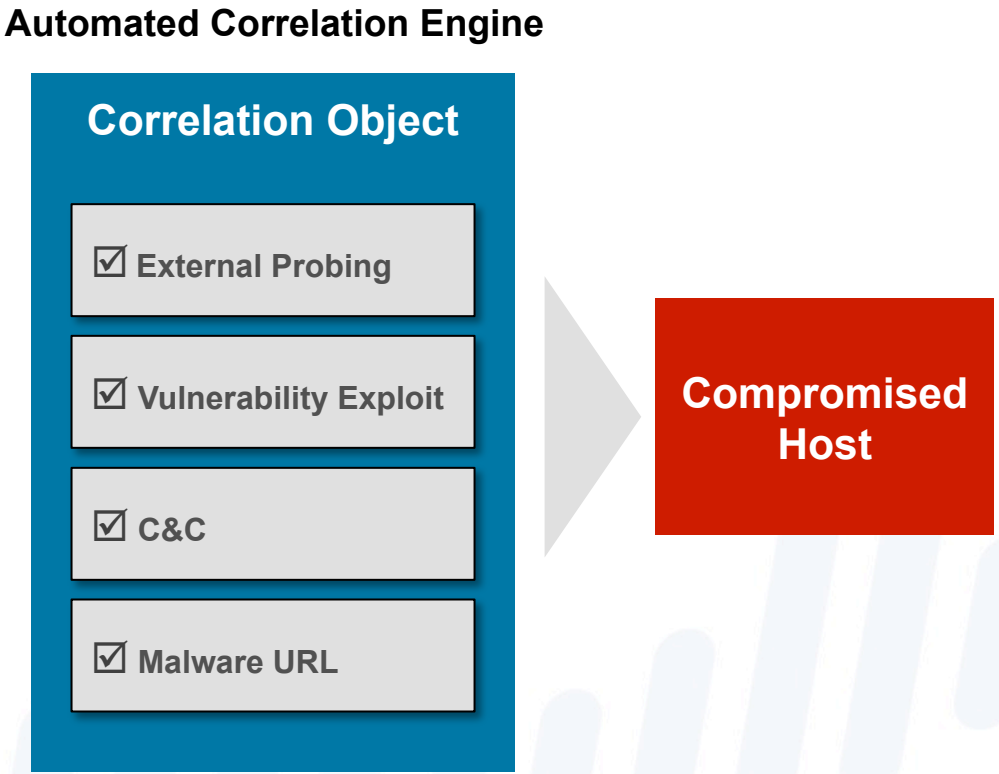
- Understand:
  - What applications are being used on the network and how that usage is changing over time
  - Who are the risky users on the network
  - Who is being targeted by attackers
  - What vectors are used to attack endpoints
  - What traffic is being successfully blocked and which rules did the blocking

Automated Correlation Engine

- Many incidents are not easily discovered or confirmed
- If there are connections between events that indicate a problem, it is left to the admin to discover
- Through the Automated Correlation Engine, higher level conclusions can be made that are more actionable

Automated Correlation Engine

- Correlation Objects look for a combination of confirmed Indicators of Compromise
- Automatically highlight compromised hosts
- Correlation Objects are defined by our Threat Research Team and updated via content

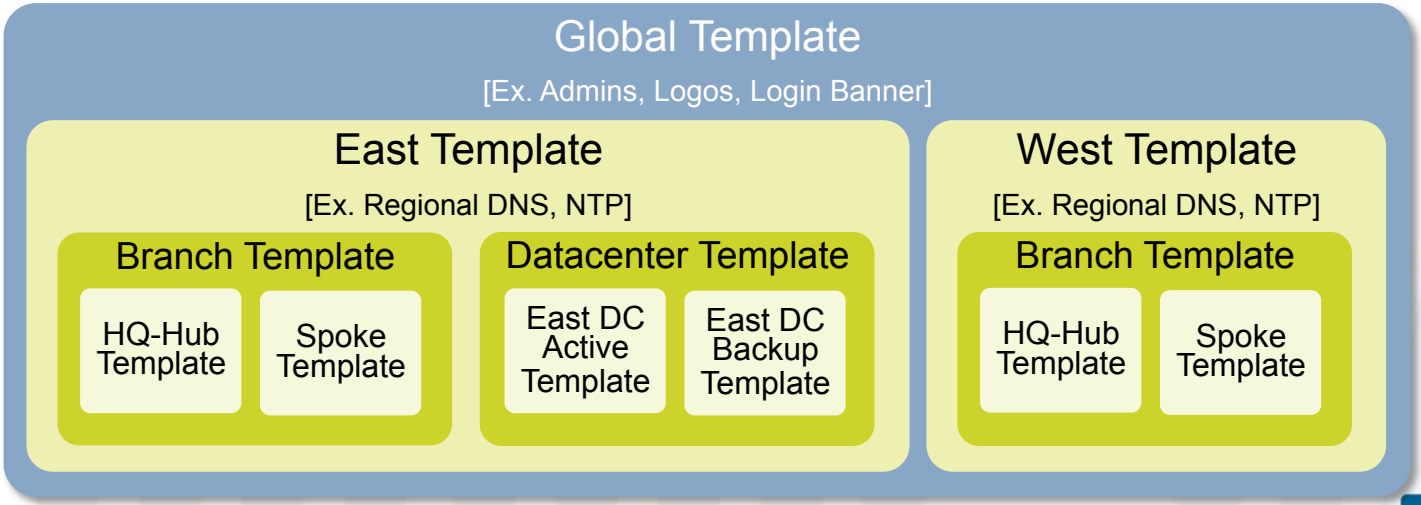


Enterprise-class management extensions

- Ability to import an existing device's configuration allows for quick sharing of existing configurations
- Moving of rules and objects to different context within the configuration
- Improved granular admin roles and access domains for device group and template admins

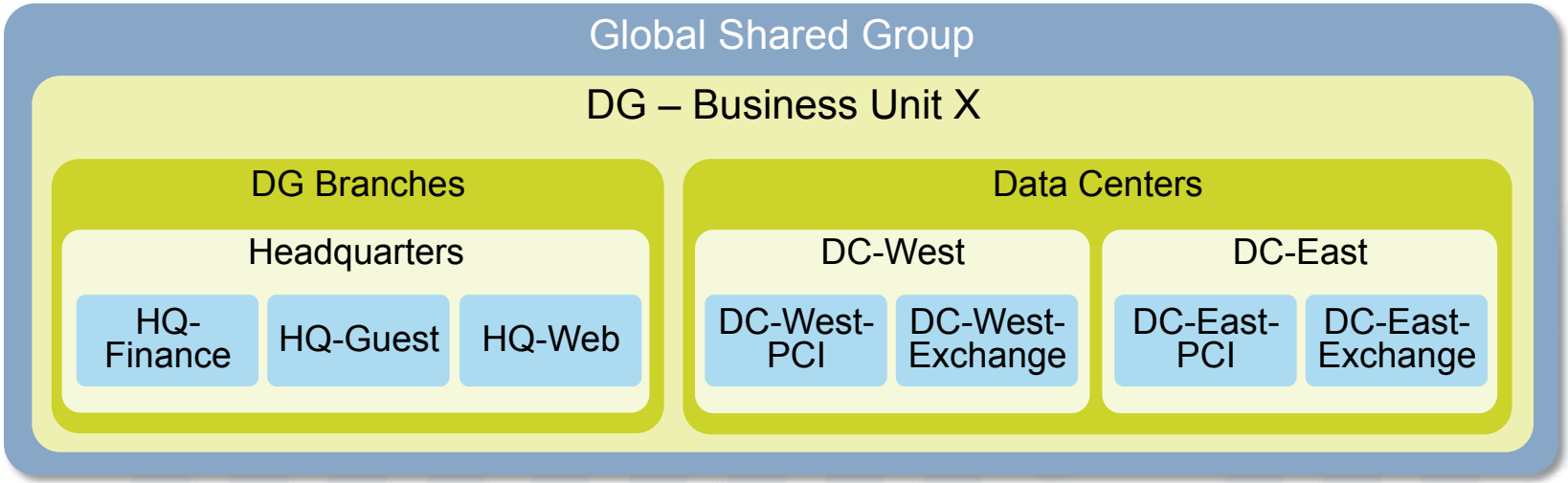
Template stacking

- Ability to stack multiple templates for device configuration allows for flexible sharing of common device settings
- Stacked templates enable global, regional, and specific network and device config
- Template Stacks will allow for complete device and network config for each device



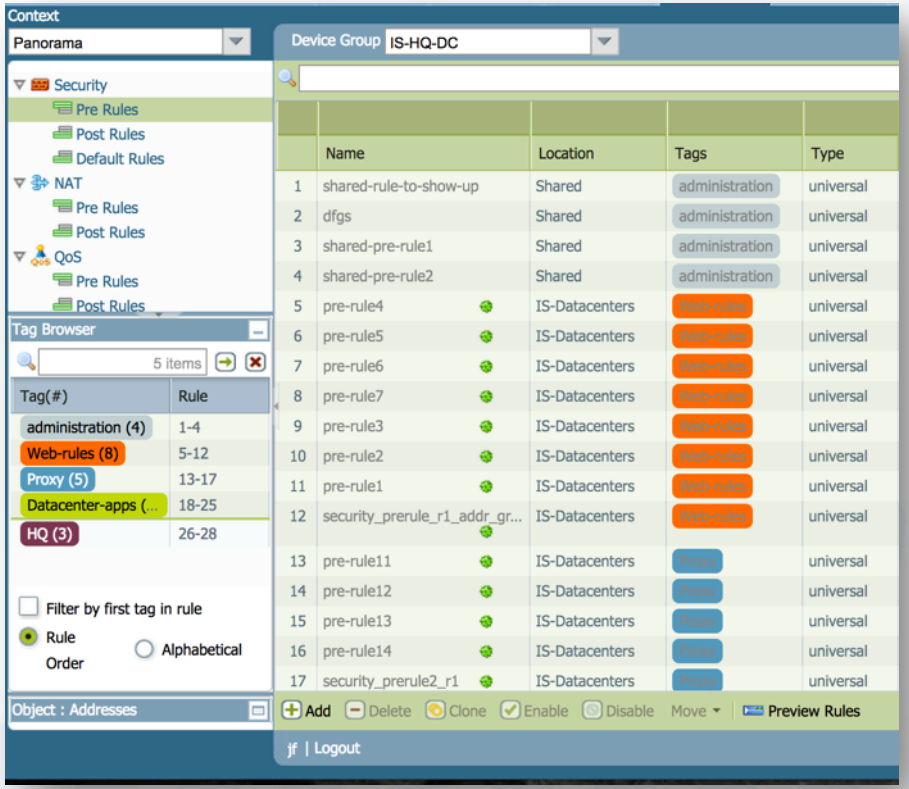
Extending device group hierarchy

- Extended device group hierarchy enables rule structure to match organizational complexity and varying levels of admin responsibility
- Extending policy hierarchy with four additional level pre/post rules for more granular rule distribution
- Granular object scoping to the most applicable device group



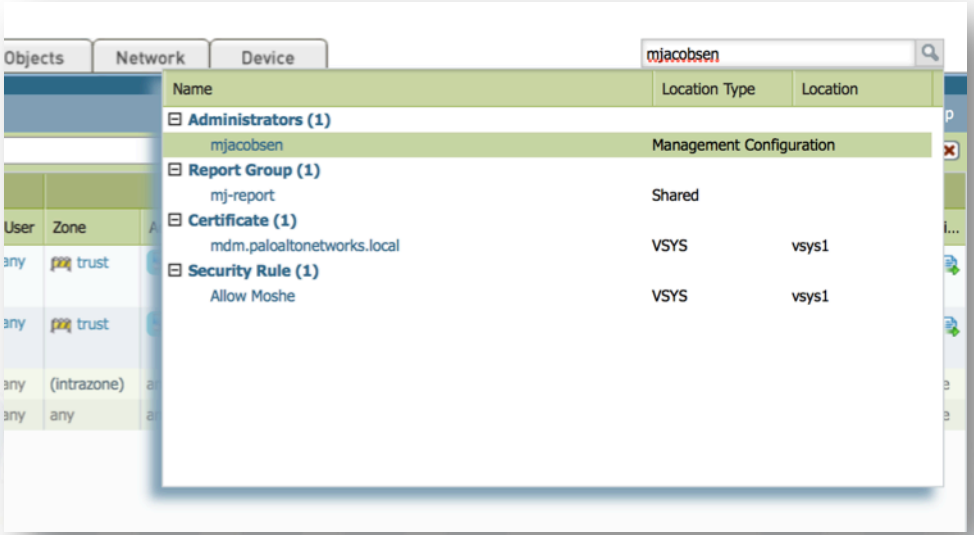
Tag-based rule grouping

- Categorize and group rules using flexible rule tagging
- More flexible and dynamic than traditional rule-grouping functionality in legacy firewalls
- Quickly view related rules, regardless of location in rulebase
- Ability to use tag structure as primary rulebase navigation mechanism



Quickly find references throughout the config

- “Spotlight”-like search of firewall config
- Preview config details
- Quickly edit the object or jump to the desired area



Contents

- Highlighted features
  - Management/Panorama
  - WildFire
  - App-ID/User-ID
  - Virtualization
  - Decryption
  - Hardware
- Summary of all other features
- Detail on the rest of the features

Malicious PDF detection

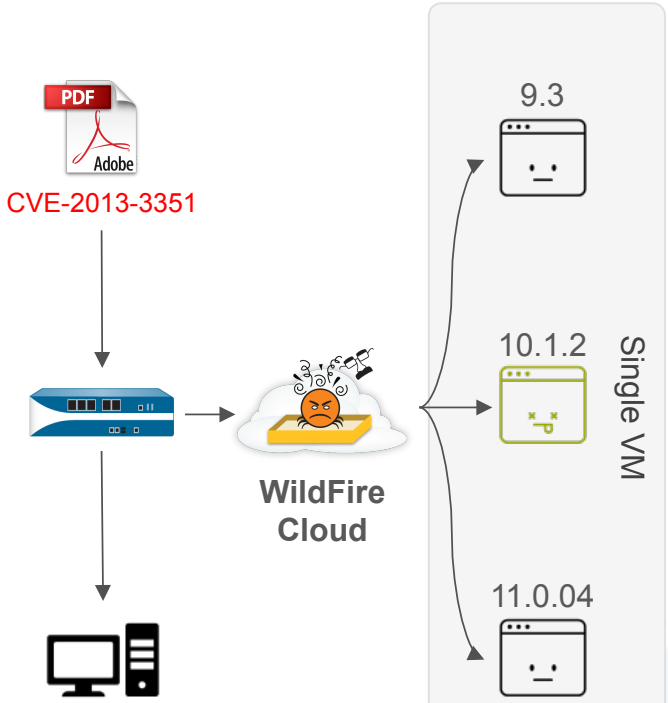
- A single version of Adobe Reader offers a limited chance of successful exploit
- Therefore, to catch malicious PDFs, its important to look across many versions of Adobe Reader

Example of Adobe Reader vulnerabilities by version:

	9.1.0	9.3.0	9.5.4	10.1.2	10.1.10	11.0.03	11.0.04	11.0.05	11.0.08
CVE-2014-0560				X	X	X	X	X	X
CVE-2014-0511				X		X	X	X	
CVE-2013-3358				X		X			
CVE-2013-3346	X	X	X	X					
CVE-2010-2883	X	X							

Multi-version analysis for PDFs

- Analyzes PDFs across multiple versions of Adobe Reader in a single virtual machine
  - Broad vulnerability coverage and exploit detection
  - Higher verdict accuracy for application-specific attacks
  - No increase in analysis time
- Reports on vulnerable versions of Adobe Reader
  - Better forensic data for analyst review and post-infection incident handling
- **Public cloud only**

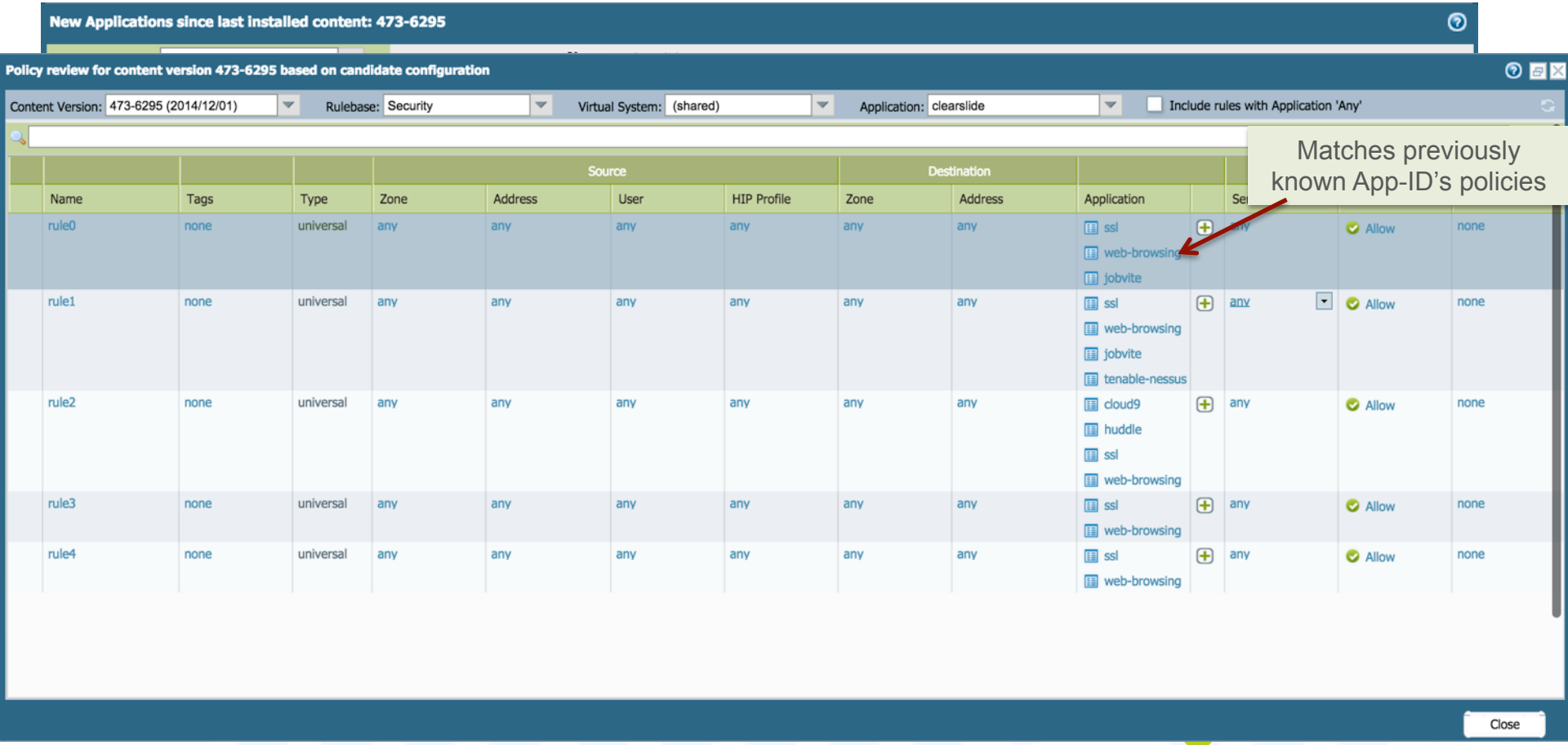


Contents

- Highlighted features
  - Management/Panorama
  - WildFire
  - App-ID/User-ID
  - Virtualization
  - Decryption
  - Hardware
- Summary of all other features
- Detail on the rest of the features

Increased workflow options for App-ID content updates

- Provide visibility into how content updates will affect policy
- Simplify the process of incorporating new App-IDs into policy
- Ability to disable new App-IDs before content install to temporarily defer policy updates


New Applications since last installed content: 473-6295
Policy review for content version 473-6295 based on candidate configuration
Content Version: 473-6295 (2014/12/01)
Rulebase: Security
Virtual System: (shared)
Application: clearslide
Include rules with Application 'Any'
Matches previously known App-ID's policies
Source
Destination
Name
Tags
Type
Zone
Address
User
HIP Profile
Zone
Address
Application
rule0 none universal any any any any any any ssl web-browsing jobvite any Allow none
rule1 none universal any any any any any any ssl web-browsing jobvite tenable-nessus any Allow none
rule2 none universal any any any any any any cloud9 huddle ssl web-browsing any Allow none
rule3 none universal any any any any any any ssl web-browsing any Allow none
rule4 none universal any any any any any any ssl web-browsing any Allow none
Close

User-based policy enforcement within proxy traffic

Apply user based policy in “north of the proxy” deployments

- Leverages the source address in HTTP header information for User-ID visibility and policy enforcement

		Source			Destination						
	Name	Zone	Address	User	Zone	Address	Application	Service	Action	Profile	Options
1	The Beatles	trust	proxy	ACME\The Beatles	untrust	any	web-browsing	application-default			
2	Everybody Else	untrust	proxy	unknown	trust	any	web-browsing	application-default		none	

Contents

- Highlighted features
  - Management/Panorama
  - WildFire
  - App-ID/User-ID
  - Virtualization
  - Decryption
  - Hardware
- Summary of all other features
- Detail on the rest of the features

Full high availability for VM-Series

- Provides session continuity when a failure occurs
- Full Active/Passive and Active/Active support for ESXi, SDX, and KVM
  - Not supported with NSX integration; limited support on AWS
- Feature parity with high availability feature set on high end appliances
- Link level detection for VM-Series vNic, not for host's physical link down
- VM-Series pair in HA should have identical hardware resources
- HA peers may be deployed on a single host or separate hosts

Usage-based pricing for Amazon AWS

- Sold and deployed directly via AWS Marketplace
  - Customer has EULA with Palo Alto Networks
  - VM-Series is pre-licensed, no need to purchase or enter an authcode
- Hourly or annual pricing available
- VM-Series capacity license with two subscription bundle options:
  - Bundle 1: Threat Prevention, Premium Support
  - Bundle 2: Threat Prevention, Premium Support, WildFire, PAN-DB URL Filtering, GlobalProtect

Active/Passive high availability in Amazon AWS

- Provides session continuity when a failure occurs
- Active/Passive supported within a single availability zone
- How it works:
  - HA1 operates on management interface
  - HA2 operates on ethernet1/1 dataplane interface
  - Makes API calls to AWS infrastructure to move (detach, attach) all dataplane interfaces (ENI's)
  - HA pair must be launched with IAM role permissions:
    - ec2:AttachNetworkInterface
    - ec2:DetachNetworkInterface
    - ec2:DescribeInstances
    - ec2:DescribeNetworkInterface
  - Failover time is typically 15-20 seconds, dictated by interface detach/attach API performance

Hypervisor assigned interface MAC

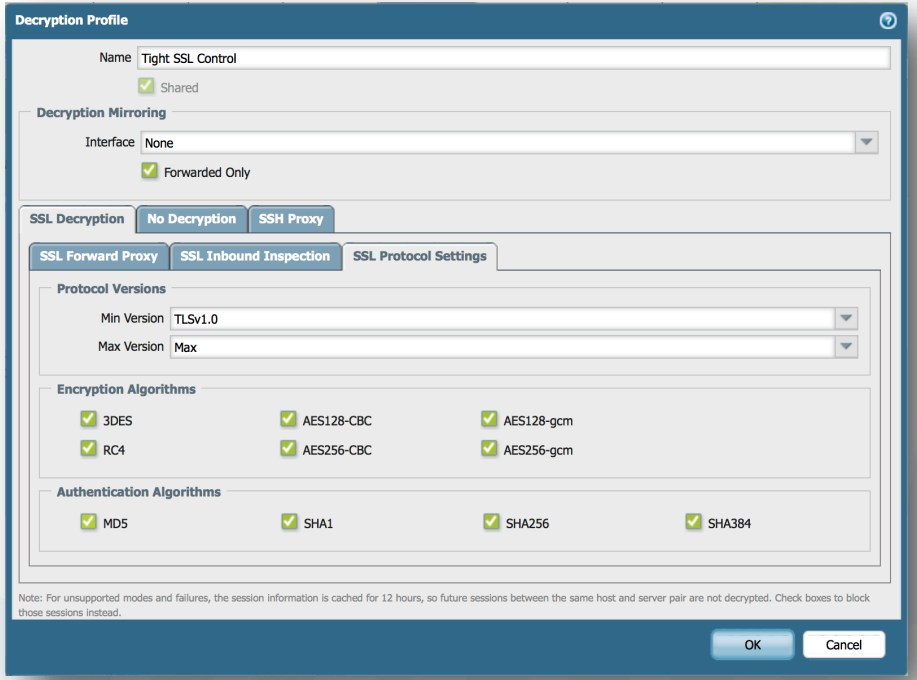
- Virtual switches don’t have capability to learn device-generated MAC
- Promiscuous mode affects performance
  - Certain cloud solutions don’t allow interface mode changes
- Solution
  - Layer 3 interface’s MAC will be assigned by the hypervisor
  - On HA failover, new active will send gratuitous ARP
- Points to Note
  - Allows VM-Series to better integrate with vCloud Air
  - No support for VLAN L3 Interfaces
  - MAC poisoning protection on guests will slow learning of new MAC after failover; we recommend disabling this protection
  - Enabled via web interface – Device > Management > Setup > General Settings

Contents

- Highlighted features
  - Management/Panorama
  - WildFire
  - App-ID/User-ID
  - Virtualization
  - Decryption
  - Hardware
- Summary of all other features
- Detail on the rest of the features

Cipher suite and protocol version control

- Improve security of decrypted SSL sessions with cipher and version control
- Stop the use of weak algorithms
- Block the use of vulnerable SSL/ TLS versions
- Supports all versions of TLS and adds support for AES GCM mode



Contents

- Highlighted features
  - Management/Panorama
  - WildFire
  - App-ID/User-ID
  - Virtualization
  - Decryption
  - Hardware
- Summary of all other features
- Detail on the rest of the features

M-500

- New management platform (higher performance and capacity than M-100)
  - 2x storage capacity
  - 8x memory
  - 2x CPU
- Hot-swap dual power supply
- Can function in three modes of operation:
  - Panorama manager (requires Panorama 25, 100, or 1,000-device license)
  - Panorama logger (requires 25-device Panorama license)
  - Or PAN-DB Private Cloud (no license required)

Comparison – M-500 and M-100 appliances

	M-500	M-100
RAM (GB)	128	16
# of CPUs	16	8
Disk Space (TB)	Up to 8TB RAID	Up to 4TB RAID
Power Supply	2	1
Comments	▪ Hot-swap dual power supply ▪ Front to back airflow	▪ Front to back airflow

New PA-7050 network processing card with 40Gig interfaces

- Provides 2 x 40Gig interfaces plus 12 x 10GigE (SFP+)
- Same performance and capacity as a PA-7000-NPC-20G
- OK to mix & match NPCs in the same chassis
- New NPC requires PAN-OS 7.0 or later to operate – will not work with earlier versions of PAN-OS

Simplified GlobalProtect licensing

- The GlobalProtect Portal license has been eliminated
  - Portals running on pre PAN-OS 7.0 versions still require the Portal license
- As with past versions of PAN-OS, the GlobalProtect Gateway subscription is required for mobile app support and HIP checks

Feature	Gateway Subscription
Single, external gateway (Windows and Mac)	
Single or multiple internal gateways	
Multiple external gateways	
HIP Checks	✓
Mobile app for iOS and/or Android	✓

Contents

- Highlighted features
  - Management/Panorama
  - WildFire
  - App-ID/User-ID
  - Virtualization
  - Hardware
- Summary of all other features
- Detail on the rest of the features

Additional PAN-OS/Panorama 7.0 features

- User-ID
  - Custom LDAP groups
- Content-ID
  - Granular action choices in threat profiles
  - One additional level of unzip/decode support
  - Ability to block when unable to fully unzip/decode
  - Negate operator for custom signatures
- WildFire
  - File analysis across WF-500 & public cloud based on file type
  - Addition of grayware analysis result
- GlobalProtect
  - Disable local subnet access
  - Static allocation of IP addresses
  - Dispatch RADIUS VSAs
  - Support RDP to remote devices
  - Option to always display welcome page
- Virtualization
  - Jumbo frame support
  - Automated license de-provisioning
- Management
  - SaaS application usage report
  - SNMP counter monitoring
  - Virtual system name reporting
  - Log deletion based on time
  - Comprehensive validate operation
  - Software upload improvements for offline networks
  - Ability to move objects
- Panorama
  - Log collector redundancy
  - Device HA status visibility
- Networking
  - ECMP
  - DHCP options
  - Virtual system-specific service routes
  - Configurable deny action
  - SNMP stats for logical interfaces
  - LLDP
  - IPv6 network prefix translation (NPTv6)
  - QoS based on DSCP
  - QoS on aggregate interfaces
- IPSec
  - IPSec IPv6 support
  - IKEv2 support
  - Single-tunnel performance improvement on PA-5000 Series
- Crypto/Authentication
  - TACACS+ authentication
  - Kerberos support
  - Enforce cipher suite and version in decryption profile
  - Control non-decrypted SSL traffic
  - TLS 1.2 support on services
  - Suite B support
  - Decryption performance improvements


paloalto
NETWORKS
the network security company™

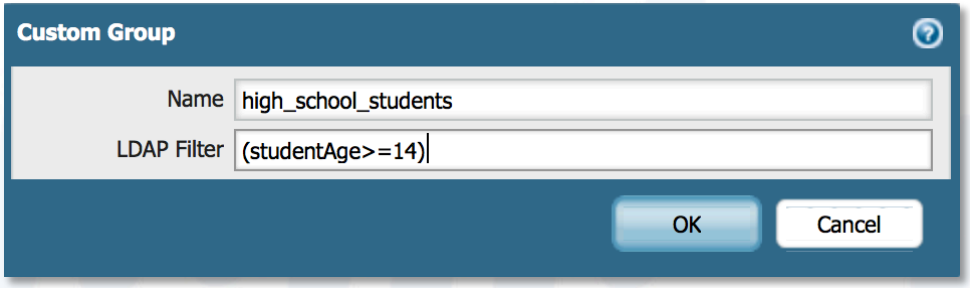
Additional features in detail

paloalto NETWORKS
the network security company™

Authentication and User-ID

Custom LDAP groups

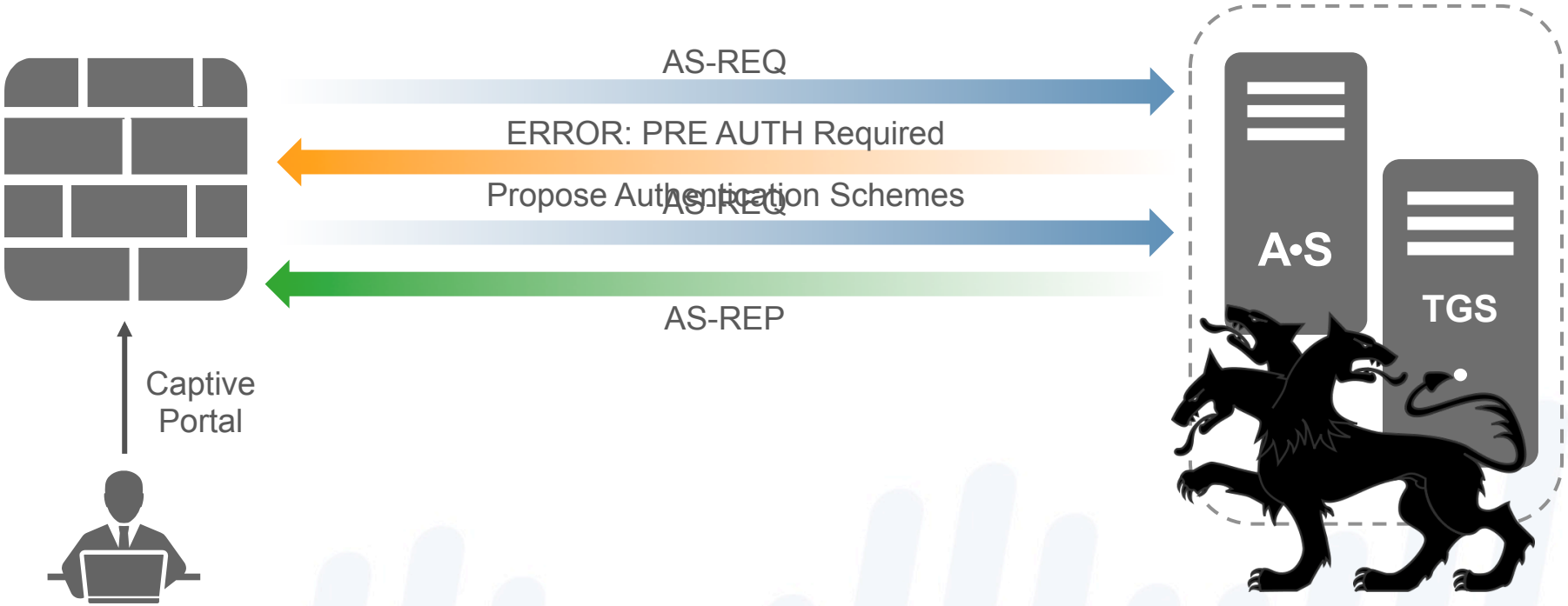
- Create “logical” group based policy where groups do not/cannot exist as LDAP groups
- Custom groups based on OU:
  - AD does not support the use of an OU’s distinguished name (DN) as a filter, so the DN is specified as the base DN in an additional LDAP server object
  - That LDAP server object is then used in the group mapping configuration, with a simple custom group LDAP filter such as (ObjectClass=person) to enumerate users
- Custom groups based on LDAP attributes:
  - Contractors vs. Employees – "employeeType=6250" vs. "employeeType=7250"
  - Students – Aged >= 14 years vs. Aged <= 14 years



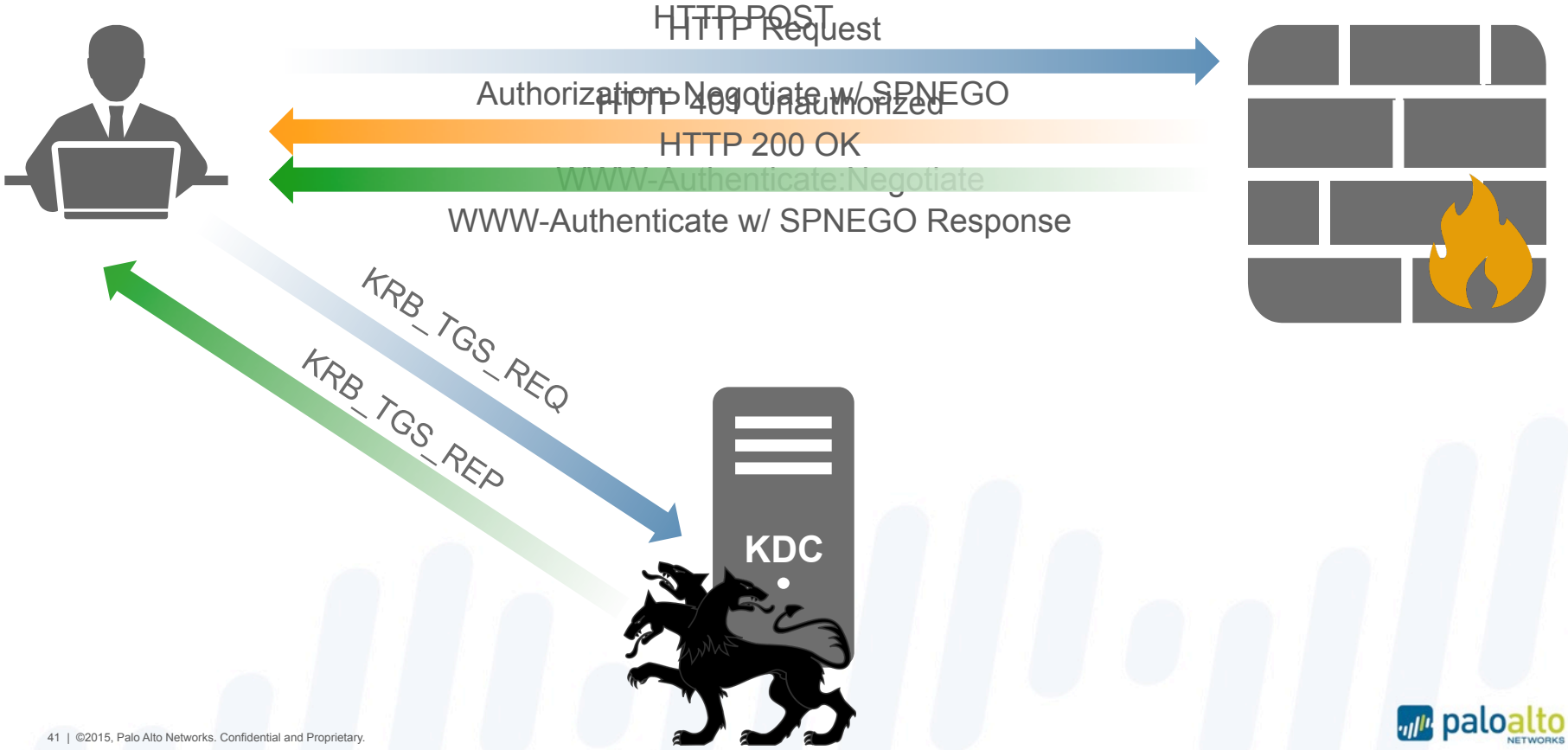
SSO with Kerberos v5

- Transparent authorization using Kerberos challenge
- Supported for Captive Portal and admin web interface for PAN-OS and Panorama
- Service principal keytab for firewall created out of band by a Kerberos admin
- Client must possess Kerberos tokens – `KRB_TGS_REQ/KRB_TGS_REP`

Authenticating users with Kerberos



Authenticating to a service with Kerberos



Kerberos authentication vs. challenge

Kerberos Authentication

- Explicit Authentication
- Triggered with a Kerberos Server Profile
- RFC Compliant `AS-REQ/AS-REP`
- Requires Pre-Authentication
- No "Token" operations – process stops at Authentication

Kerberos Challenge

- Transparent Authorization
- Decrypt & Verify Kerberos Ticket
- `WWW-Authenticate:Negotiate`
- Service Principal Keytab must be created out-of-band by a Kerberos Administrator
- The client needs to possess Kerberos tokens → `KRB_TGS_REQ/KRB_TGS_REP`

TACACS+ authentication

- TACACS+ authentication supported for better authentication flexibility
  - Authorization and accounting are not available at this time
- Administrators can use TACACS+ to logon to the web interface & CLI
- TACACS+ is also available for use as an authentication scheme for Captive Portal and GlobalProtect

Authentication troubleshooting tools

- Test Settings … On **CANDIDATE** Configuration
- Verify:
  - Network connectivity
  - Shared secrets/admin accounts
  - Allow list checks
  - Returned VSAs
- Considerations:
  - Uses committed service routes
  - Commands must be run on the authenticating device

```
admin@pm-firewall(active)> test authentication
vsys vsys1 authentication-profile "LDAP
Authentication Profile" username amurthy
Enter password :

Do allow list check before sending out
authentication request...
name "amurthy" is in group "all"
Authentication to LDAP server at pa-
dc-1.paloaltonetworks.local for user "amurthy"
Egress: 10.47.0.20
Type of authentication: plaintext
Starting LDAP connection...
Succeeded to create a session with LDAP server
DN sent to LDAP server: CN=Ashwath Murthy,OU=Santa
Clara,OU=Users,OU=PAN,DC=paloaltonetworks,DC=local
User expires in days: never

Authentication succeeded for user "amurthy"

admin@pm-firewall(active)>
```


Virtualization

Jumbo frames support for VM-Series

- Jumbo frames now supported to improve performance in datacenter environments
  - App-ID throughput on 64KB HTTP transaction test has **doubled**
  - Threat prevention throughput on the same test has **increased by 50%**
- Enable jumbo frames globally - Device > Setup > Session > Session Settings
- Note:
  - Doesn't apply to NSX VM-Series due to hypervisor level Integration
  - Not supported on Citrix SDX

Licensing and auth-code enhancements

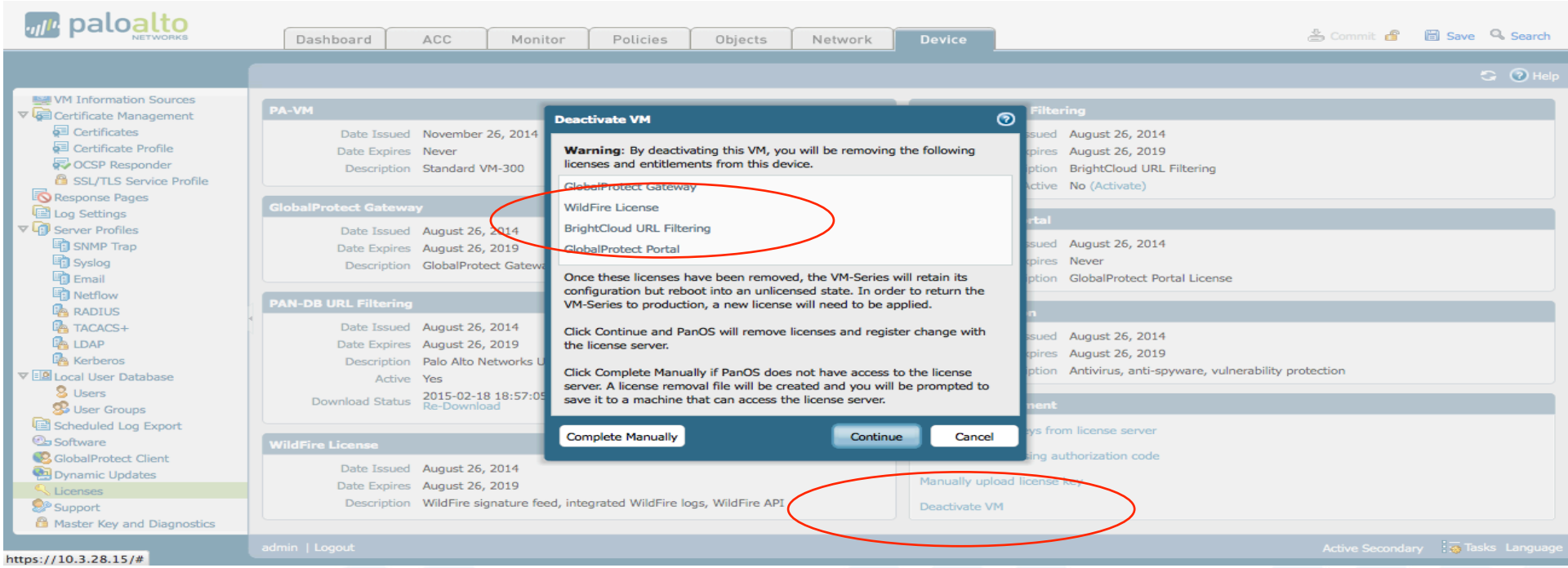
- Mistakes made during the license assignment process are difficult to correct
- Moving a VM-Series capacity license requires interaction with customer support
- Move subscriptions between devices (Hardware or VM-Series)
  - Self-service ability to move subscription when it was assigned to the wrong device
  - New deactivate key command from CLI will free up auth-code to be re-applied
- De-activate and re-deploy VM-Series license
  - Self-service ability to deactivate a VM-Series appliance and free up **all** license and subscription auth-codes to be re-applied
  - Initiated from web interface/CLI/API in PAN-OS for single or Panorama for bulk
- Time based capacity license for VM-Series
  - If present, VM capacity license will now honor an expiration date
  - If expired, VM-Series will continue to operate but will not accept software or content updates

Subscription deactivation via CLI on hardware

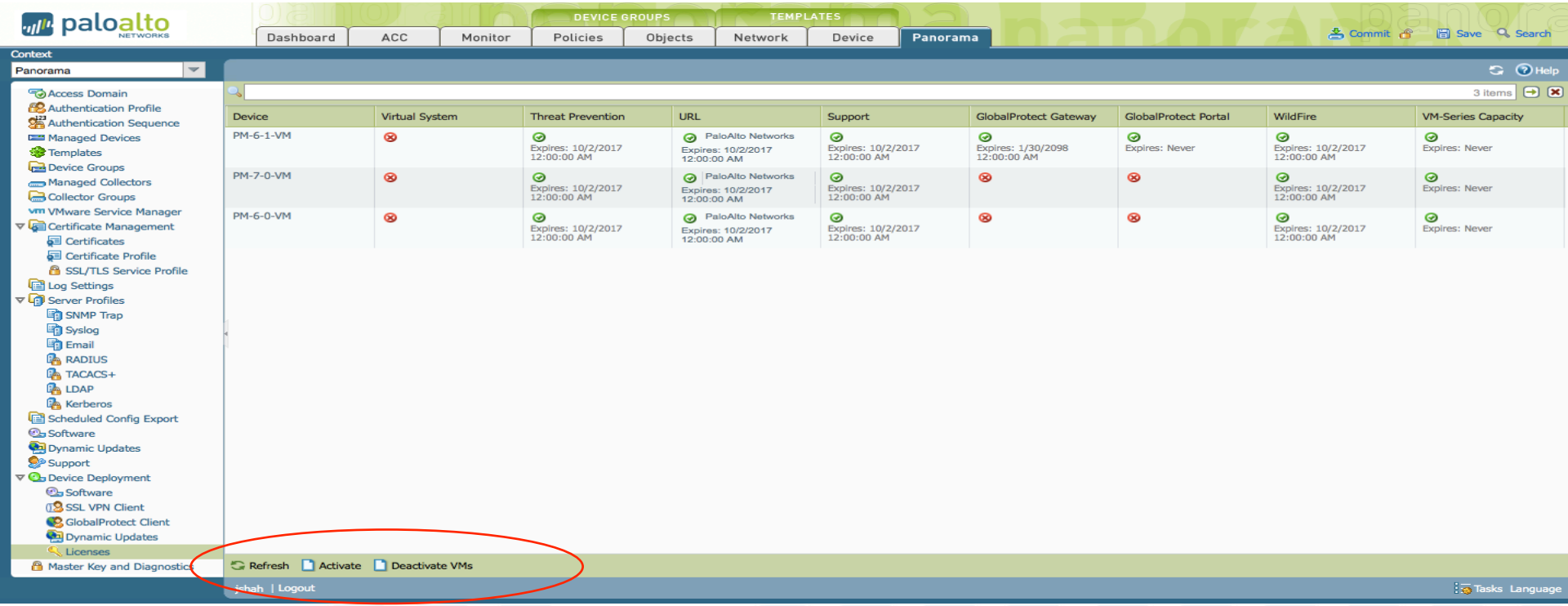
```
admin@5060-1(active-primary)> request license deactivate key features
  [                                                 Start a list of values.
  BrightCloud_URL_Filtering_2014_08_12_I5463528.key 2014/09/08 11:16:01        0.3K
  GlobalProtect_Gateway_2014_08_12_I7974290.key     2014/09/08 11:16:00        0.3K
  PAN_DB_URL_Filtering_2014_08_12_I2054873.key      2014/09/08 11:16:00        0.3K
  Threat_Prevention_2014_10_09.key                  2014/11/01 01:24:07        0.3K
  VirtualSystems_2014_08_12_I7238815.key            2014/09/08 11:16:01        0.3K
  WildFire_License_2014_08_12_I4791969.key          2014/09/08 11:16:01        0.3K
  <value>                                           member value
```

```
admin@5060-1(active-primary)> request license deactivate key features BrightCloud_URL_Fi
ltering_2014_08_12_I5463528.key mode auto

0008C101940  BrightCloud URL Filtering  Success

Successfully removed license keys
```

De-active VM via PAN-OS UI for single device



De-activate VM via Panorama UI for single/bulk devices

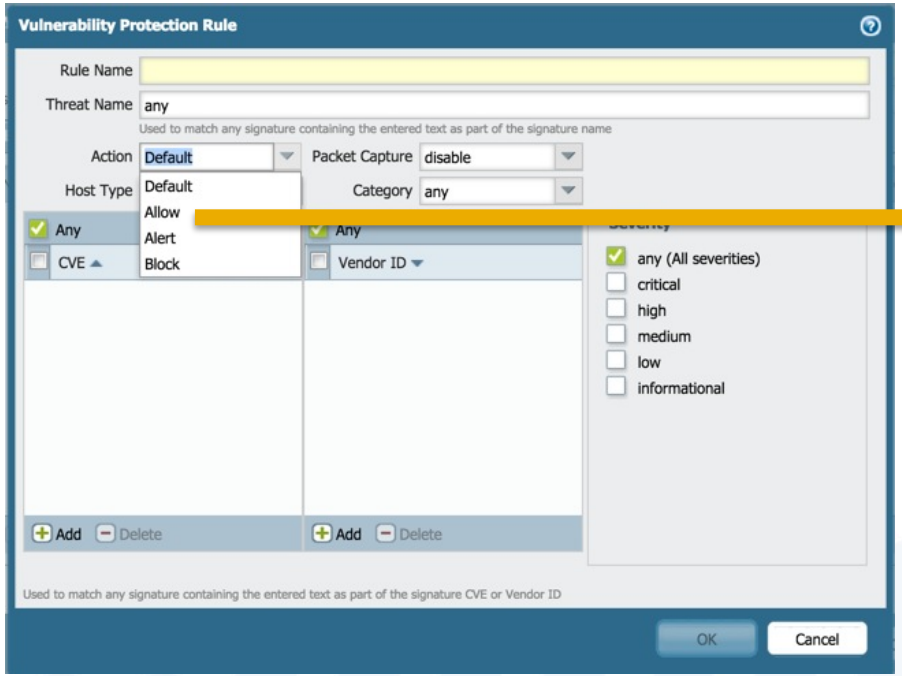


Threat Prevention and WildFire

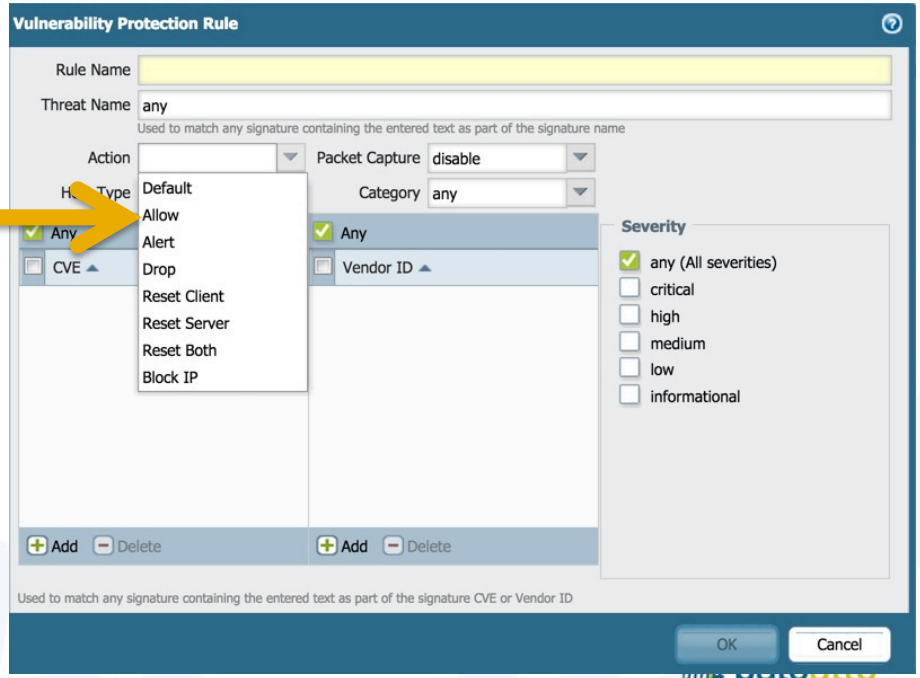
Complete action list in vulnerability protection profiles

Provides fine-grained control over session handling when threats are detected

Vulnerability profile in PAN-OS 6.0



Vulnerability Profile in PAN-OS 7.0

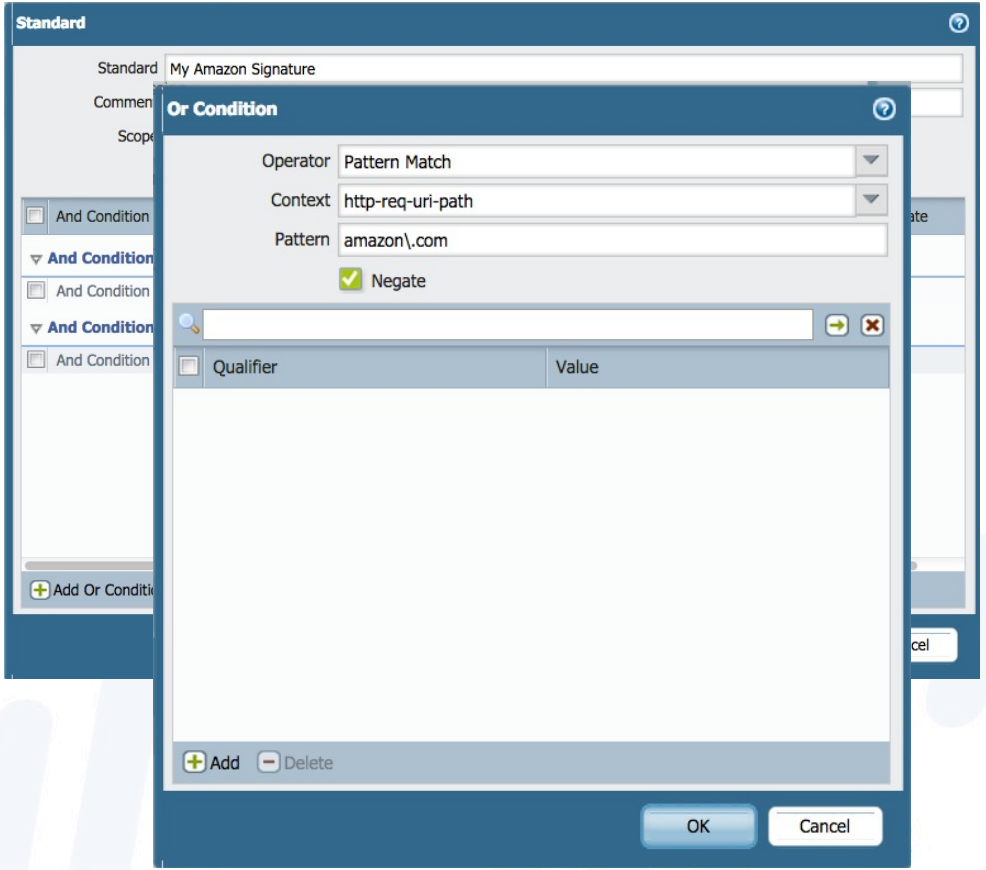


Support for additional levels of zip/compression

- Multi-level zip/compression is sometimes used to try and avoid content scanning by security devices
- Zip/compression decoding depth has been increased to four levels
  - Any combination of decoding – Zip, gzip, base64, chunked, uuencode
- Beyond four levels, files can be blocked using “Multi-level encoding” in the file blocking profile
- Example of three level compression – An Office 2007 MS Word document that has been zipped and is sent via HTTP chunked with gzip

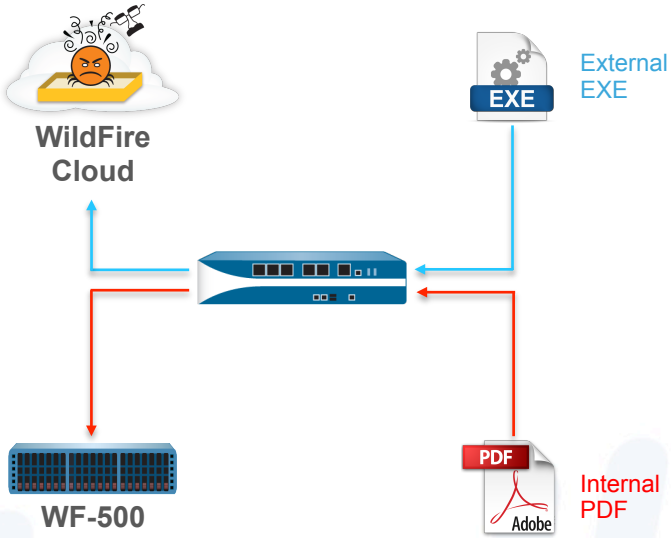
Negate operator in custom signatures

- Negate patterns in vulnerability or spyware signatures in order to create more precise threat prevention
- Example: Match a portion of a URL, such as ”redirect", but only when the host name does NOT contain "amazon.com”



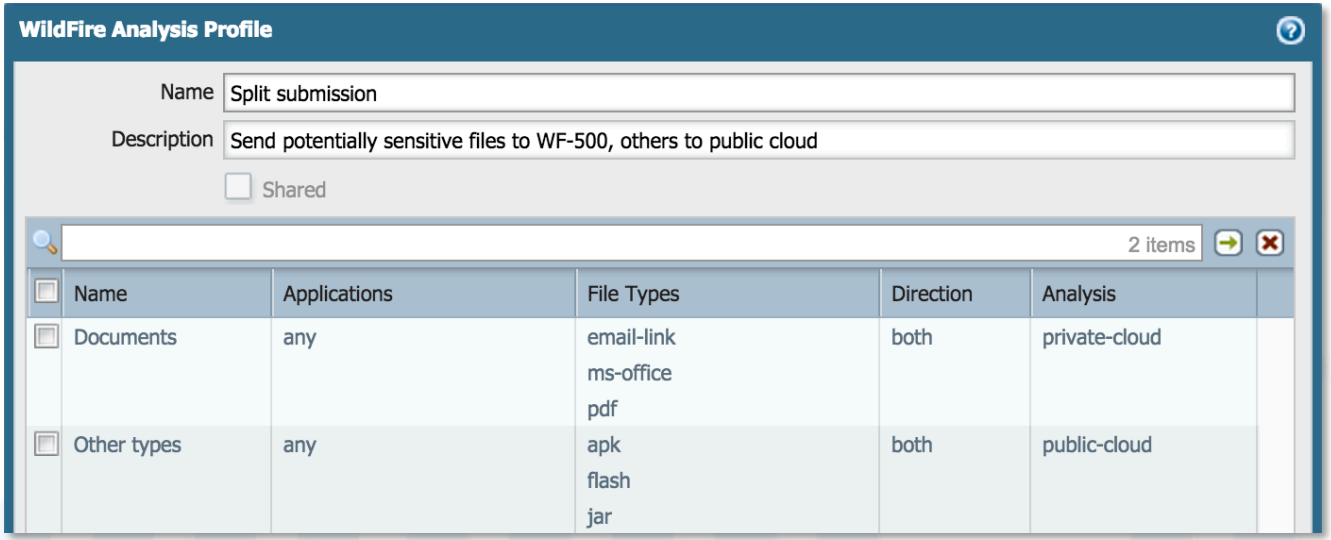
WildFire hybrid cloud

- Policy-based controls combine public cloud and local WF-500 appliance to address sensitivities related to sending certain file types off network
- Forward file types more likely to contain sensitive data to the local WF-500
- Forward external files, software packages, and Web content to the public cloud
- Analysis location is configurable by file type, application, direction of traffic, and all other security policy match criteria



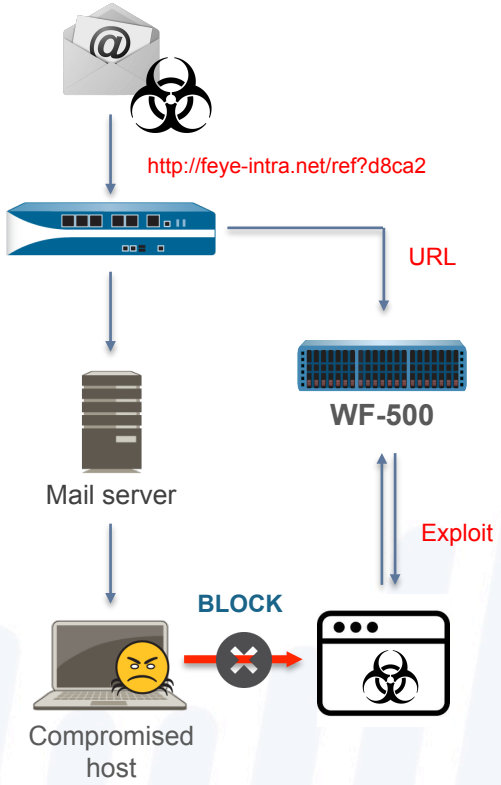
WildFire analysis security profile

- New WildFire analysis security profile simplifies file submission
- WildFire forwarding actions have been moved from the file blocking profile to the WildFire analysis profile, which can be attached to a security rule to provide the same granularity of control
- Don’t forget that the file-blocking profile is very important for blocking files types that simply shouldn’t be allowed in/out of a network due to likelihood for potentially malicious content



Email link following for private cloud

- Identify and protect against malicious email links
- PAN-OS firewalls send web links in suspicious emails to WildFire
- WildFire visits the webpage and analyzes the traffic to detect exploits and malware
- Prevent patient-0 from getting compromised by sending the URL to firewalls within 5 minutes of analysis
- Quickly identify targeted users and machines via email headers and integration with User-ID
- SMTP and POP3 supported



Additional WildFire enhancements

- New Grayware verdict distinguishes potentially unwanted programs like adware from genuine malware for better incident triage and resource allocation
  - Available in log forwarding profiles and WildFire submission logs
- More than 50 new static and dynamic analysis behaviors provide additional context for each threat analyzed
- get/verdict(s) and submit/link(s) API methods allow individual and bulk querying of sample verdicts, as well as submission of URLs for analysis. WildFire cloud only.

GlobalProtect

Disable local subnet access

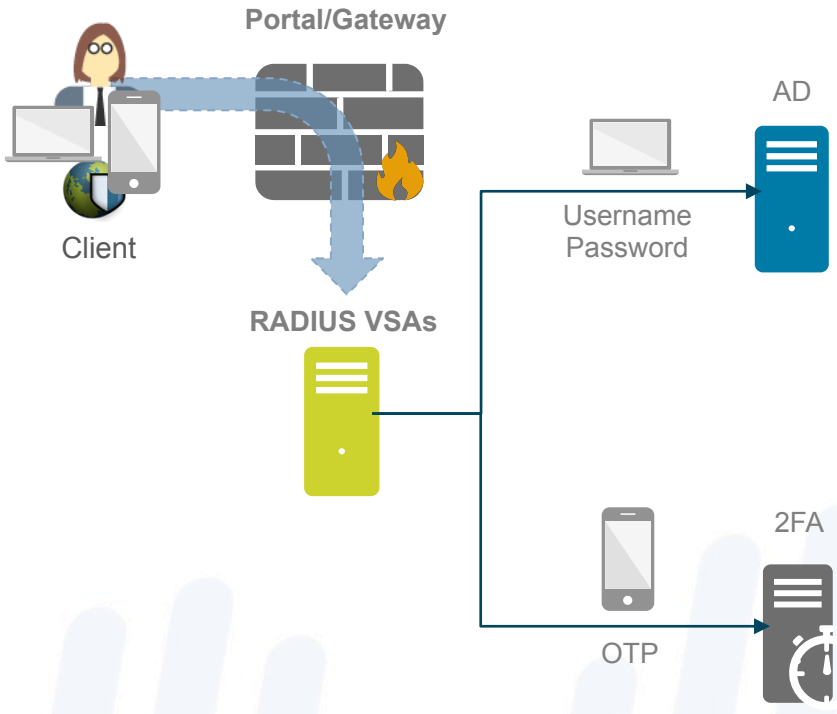
- Local subnet access for remote users carries risks because such traffic bypasses the enterprise's security policy
- All traffic will pass through the GlobalProtect gateway and be subjected to policy enforcement
- Access to resources on the local subnet (such as printers) will be blocked
- Configured on the GlobalProtect gateway
- Note:
  - Windows and Mac only
  - IPv6 traffic will not be blocked or routed through the tunnel

Static IP address allocation

- For accounting and legacy access control reasons, some networks require remote users to utilize a consistent IP address
- Static IP allocation can be achieved in two ways
  - The gateway can now maintain a mapping between the endpoint and IP pool entry for consistent IP address assignment
  - For more regimented IP address assignment, the firewall can now use the framed IP attribute from the authentication server (RADIUS or LDAP) to repeatedly assign a consistent IP address

New RADIUS VSAs

- Provides endpoint context to third-party RADIUS & 2FA systems
- VSAs GlobalProtect can dispatch:
  - Client OS
  - Hostname
  - Source IP
  - User Domain
  - GP version
- Allows discrete authentication of clients, for example:
  - Authenticate a mobile device using 2FA
  - Authenticate a laptop using username/ password



Additional GlobalProtect enhancements

- Support RDP to remote devices
  - Allows users, such as IT helpdesk, to RDP from within enterprise networks to a remote client device that has a VPN tunnel setup to a GlobalProtect gateway
  - Remote admin must login to GlobalProtect agent within configured timeout
  - User identity (for policy enforcement purposes) will then match that of the remote administrator while they are logged in on the remote device
- Option to always display welcome page
  - Provides an opportunity to display important information such as terms and conditions that may be required to meet compliance requirements
  - Forces the welcome page to be displayed with each Portal login

Management

SaaS application usage report

	App Sub Category	Application Name	Bytes	Sessions	Threats
1	file-sharing	rapidshare	30.5G	706	0
2		skydrive-base	46.9M	2.1k	0
3		docstoc-base	36.5M	725	0
4		google-drive-web	28.5M	174	0
5		sourceforge-base	758.5k	528	0
6		dropbox	478.2k	96	0
7		office-live	300.9k	96	0
8		mendeley-base	293.9k	96	0
9		hightail-base	153.6k	144	0
10	social-business	blackboard	9.0G	212.2k	2.0k
11	email	gmail-base	3.8G	59.0k	117
12		yahoo-mail	1.4G	51.5k	0
13		gmail-enterprise	573.9M	12.9k	11
14		comcast-webmail	125.3M	4.1k	0
15		aim-mail	109.7M	6.3k	0
16		facebook-mail	18.1M	1.8k	0
17		gmx-mail	4.4M	816	0
18		naver-mail	2.4M	672	0
19		netease-mail	1.5M	96	0
20		outlook-web-online	910.9k	144	0
21	internet-utility	google-analytics	264.7M	42.6k	207
22		icloud-base	37.6M	6.9k	0
23		yahoo-web-analytics	483.5k	144	0
24	office-programs	google-docs-base	147.2M	10.0k	0

Export to PDF | Export to CSV | Export to XML

Custom Reports

Application Reports

- Applications
- Application Categories
- Technology Categories
- HTTP Applications
- SaaS Application Usage
- Denied Applications

Traffic Reports

Threat Reports

URL Filtering Reports

PDF Summary Reports

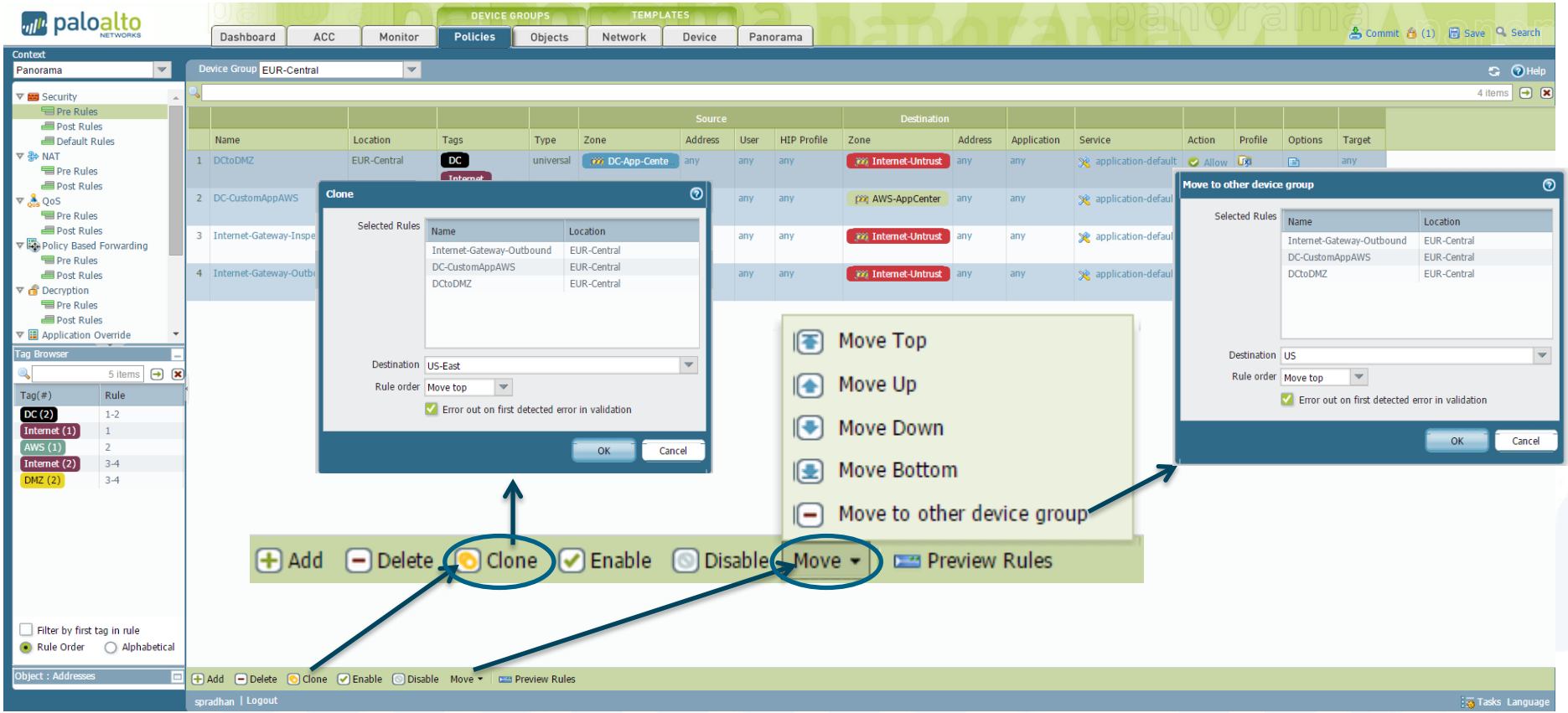
June 2015

S	M	T	W	T	F	S
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11

Move and clone objects and rules

- Use cases
  - I created the rules in the wrong DG/VSYS. Do I need to recreate all of them again?
  - I created an object as a shared object, but wanted to create it in a DG. Do I have to perform surgery on the XML config file?
  - I imported a device configuration and now want to move the lab tested rules to production
- Easy to use copy/paste (Clone) and cut/paste (Move) options
- Works with single or multiple entries

Move/clone objects and rules

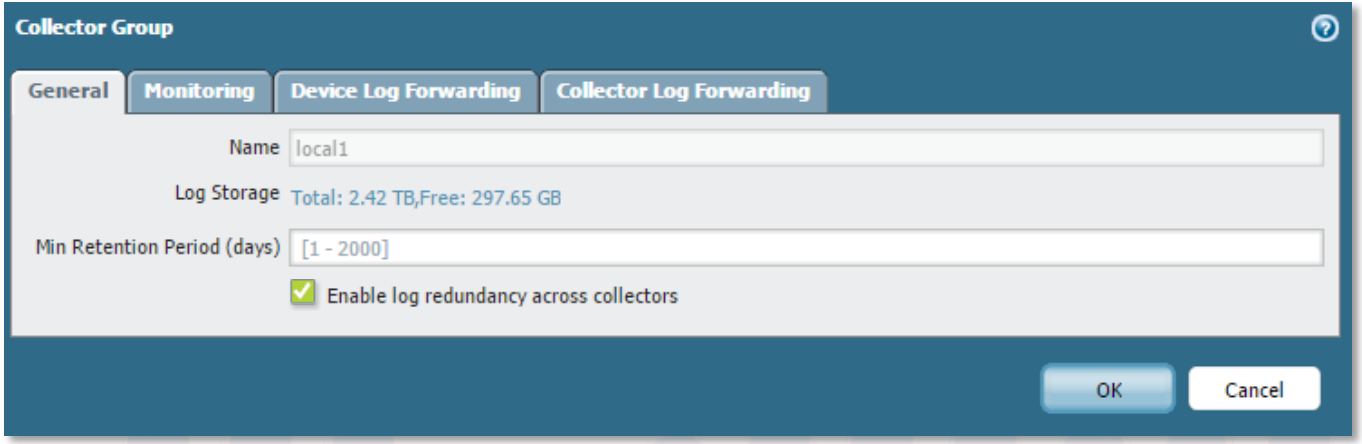


Enhanced configuration validation

- Syntactic and semantic config validation eliminates surprises during maintenance windows
  - Shows all errors at validation time, not just the first error
- Significantly improves confidence in commit being successful
- App dependencies and rule shadowing visible prior to commit
- Access control on validation across Panorama, VSYS, DG and Template

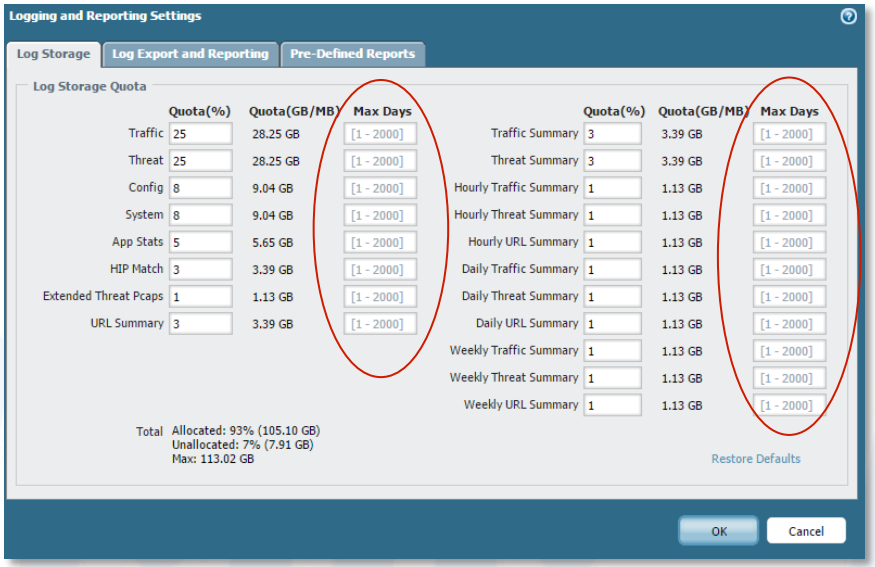
Log collector redundancy

- Store two copies of each log on devices in the collector group to eliminate log loss when a collector is lost
  - Logs will remain accessible for reporting functions following a collector failure
  - If a failed device is replaced, the same logs will be replicated to its replacement



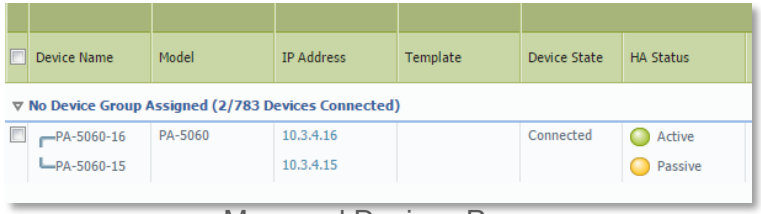
Log retention

- Regulations in certain geographies require purging of certain log types after they have been stored for a predetermined length of time
  - Log storage quotas may also require adjustment to ensure that logs will fit on disk
- Provides the flexibility to define log retention periods per log type

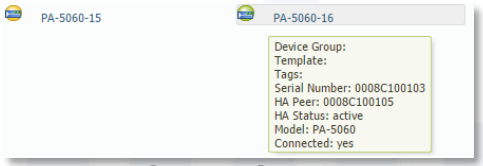


Device HA status in Panorama

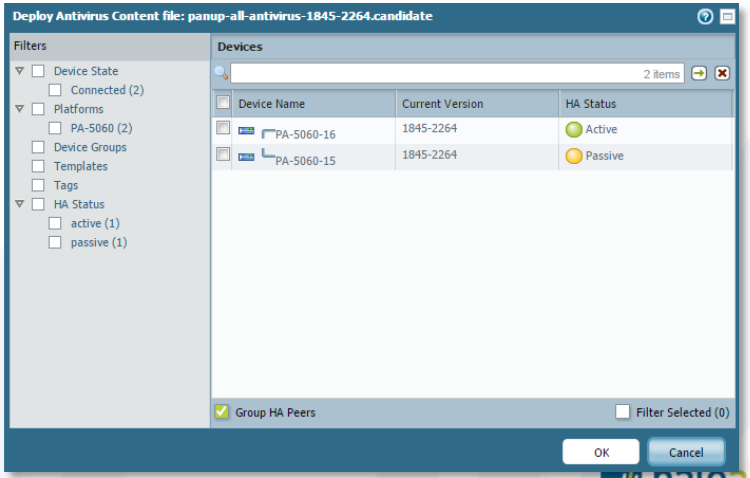
- Simplify device-level functions by quickly identifying and accessing the active firewall during a context switch
  - Access the active firewall for live troubleshooting purposes
  - Install software on the passive firewall first
- Also available in the managed devices, commit, and content update areas



Managed Devices Page



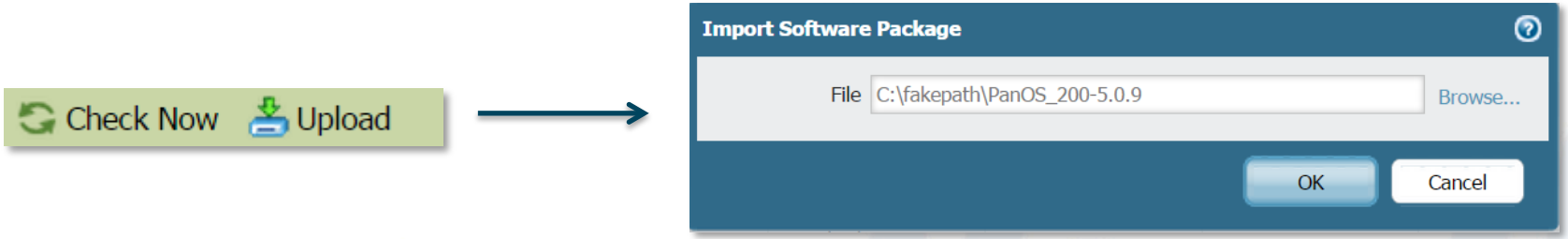
Context Switch



Deploy Content Update

Software upload for offline networks

- Standardizes software installation process regardless of how the software image was loaded onto the firewall or Panorama instance
  - Software images uploaded manually are now available for install from the available image list on the Device > Software, Panorama > Software, and Device Deployment > Software web interface screens



SNMP features

SNMP counters for logical interfaces

- L2/L3 subinterfaces
- Tunnel (including status of IPSec tunnels)
- VWire
- Aggregate ethernet (802.3ad)
- Loopback
- VLAN

- Interfaces and ifMIB
  - ifXTable and ifStackTable MIB support

- Logical interface counters and supporting tables are not supported on the PA-2000 Series or PA-4000 Series

- Global Counters (subset of “show global counters” CLI command)
  - DoS related counters
  - IP Fragmentation counters
  - TCP state related counters
  - All relevant packet drop counters

- LLDP MIB implementation (based on MIB for IEEE 802.3AB-2009)
  - Configuration
  - Neighbor information
  - Statistics

VSYS/device name support in reporting functions

- Virtual system names are now supported in reporting functions to clarify the report's context
  - Include the virtual system name in report data
  - Group by virtual system name to easily compare across virtual systems
  - Filter based on virtual system name to produce virtual system-specific reports
- In Panorama, include device name in above reporting functions

Custom Report

Report Setting | Traffic by VSYS

	Virtual System Name	Virtual System	App Category	App Sub Category	Application Name	Risk	Sessions	Threats
1	main	vsys1	networking	encrypted-tunnel	ssl	4	4	0
2		vsys1	business-systems	general-business	pan-db-cloud	1	2	0
3		vsys1	business-systems	general-business	paloalto-wildfire-cloud	1	7	0
4		vsys1	networking	infrastructure	snmp-trap	3	15	0

Networking

Equal cost multipath (ECMP)

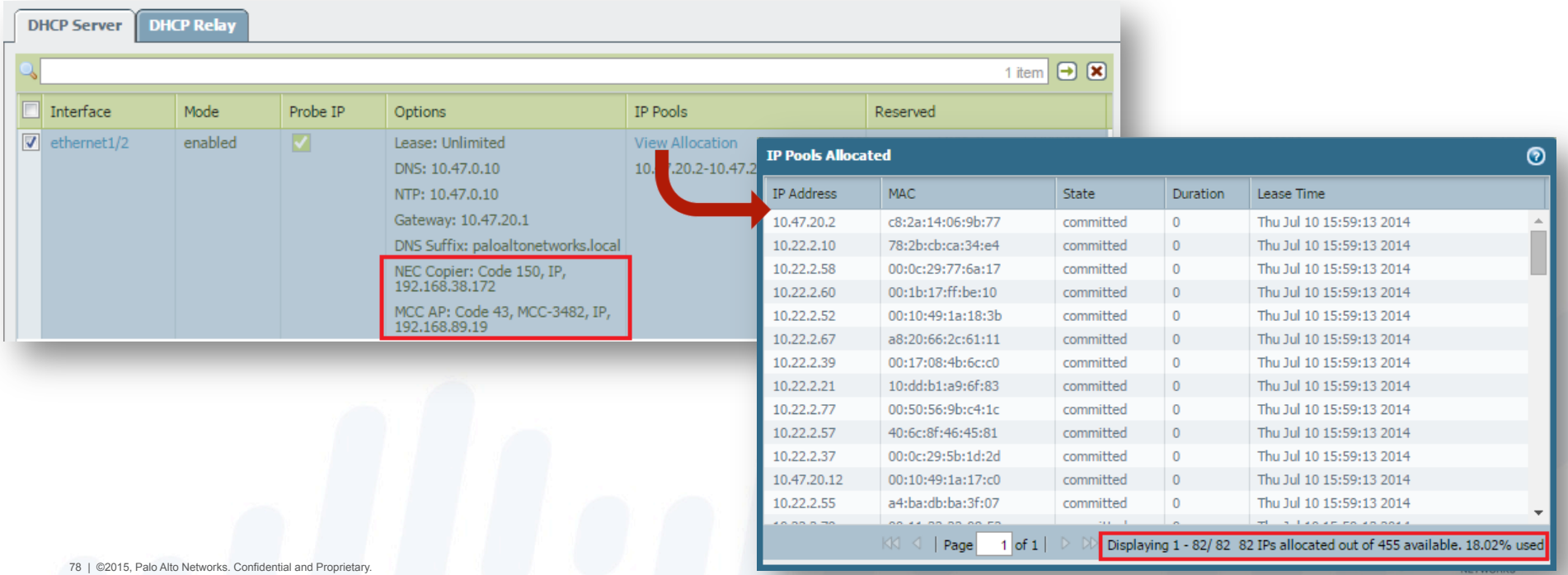
- Improves throughput, redundancy, and convergence times
- Provides support for up to 4 different paths as learned through static routes, OSPF, BGP, or RIP
  - BGP multiple AS configuration supported
- Session-sticky load sharing means a session will always take the same path
  - Load share based on src/dst IP modulo, src/dst IP and port hash, or weighted/ balanced round robin
- Inter-VR routing, multicast PIM, and LSVPN routes do not support ECMP
- Symmetric return option routes reverse flows out their original ingress interface to simplify deployment of stateful devices like DLP

DHCP options

- Simplifies branch office deployments where firewall can provide DHCP options to configure wireless access points, VoIP equipment, printers, etc.
- Flexible configuration supports all possible DHCP option codes, types, and lengths up to 255 octets
- Supports sending multiple options of a given code and multiple option codes
- Inheritance allows the firewall to forward options it learns via a DHCP client interface on to endpoints using the firewall as a DHCP server
  - Note: For options carrying IP addresses, only the first address can be inherited

Enhanced DHCP usage and statistics

- DHCP options displayed in the DHCP server summary table
- DHCP server IP pool utilization is displayed alongside IP allocation



Virtual system specific service routes

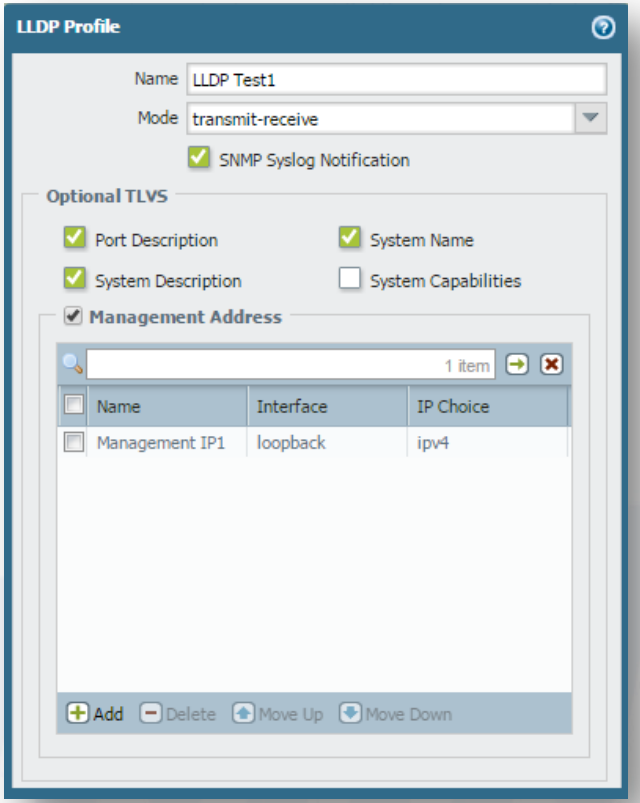
- Vastly simplifies the integration between the firewall and tenant-supplied services in multi-tenant deployments
  - E.g. Tenant supplied DNS can be used to resolve FQDN address objects for accurate security policy
  - E.g. Tenant supplied email servers can be used to email reports to stakeholders within tenancy
- Service routes are global (for device functions or virtual systems with no service routes) or virtual system-specific
- Services supported per VSYS:
  - Email
  - Kerberos, LDAP, RADIUS
  - TACAS Plus
  - Netflow
  - SNMP Trap (IPv4 only)
  - Syslog
  - UID Agent
  - VM Monitor
  - DNS
- PA-7050 uses log processing card subinterfaces to provide per-tenant log forwarding

Configurable deny action

- Provides full control over how a session is terminated by the firewall
  - Prevent client from *hanging* during session timeout
  - Preserve server's session table through reset-server
  - Silently drop attack traffic without tipping off attacker
- Security policy deny actions:
  - Deny — Retains current behavior (App-ID-specified action of drop or reset)
  - Drop — Silent drop, App-ID's action is not taken
  - Reset Client — TCP RST to client
  - Reset Server — TCP RST to server
  - Reset Both — TCP RST to both client & server

Link layer discovery protocol

- LLDP simplifies network discovery and topology mapping
- IEEE 802.1AB LLDP device discovery uses layer 2 communications to learn identifying information about layer 2 neighbors
  - Chassis ID, Port ID, TTL
  - Port Description
  - System Name, System Description
  - System Capabilities
  - Management Address
- Supports standard IEEE802 LLDPv2 MIB
- Controlled globally in conjunction with LLDP profiles on the interface level
- Supported on L2, L3, and virtual wire interfaces
- All platforms except PA-2000 Series supported

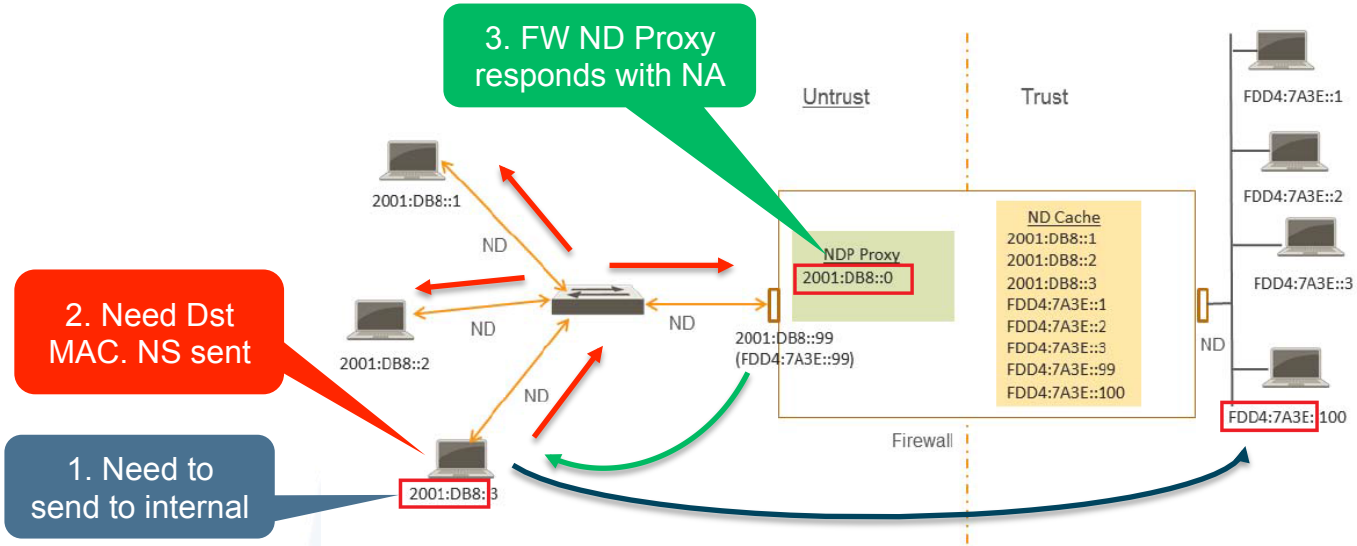


Network prefix translation (NPTv6)

- Facilitates address independence – prefix changes don't have to impact internal addressing
- Stateless prefix translation conforming to RFC 6296
  - Translate prefix from 32 to 64 bits
  - Only static translation for source/destination/u-turn NAT
- IP header **must** generate same pseudo-header checksum before/after translation
  - Packets with checksum neutral math = 0xffff, are dropped (per RFC)
  - Helper commands provided to calculate host address outside the firewall
- PAN-OS 7.0 ALG support - Oracle, RTSP, FTP
- Limitations
  - Does not provide port translation (dynamic IP/port) or host translation as with NAT66

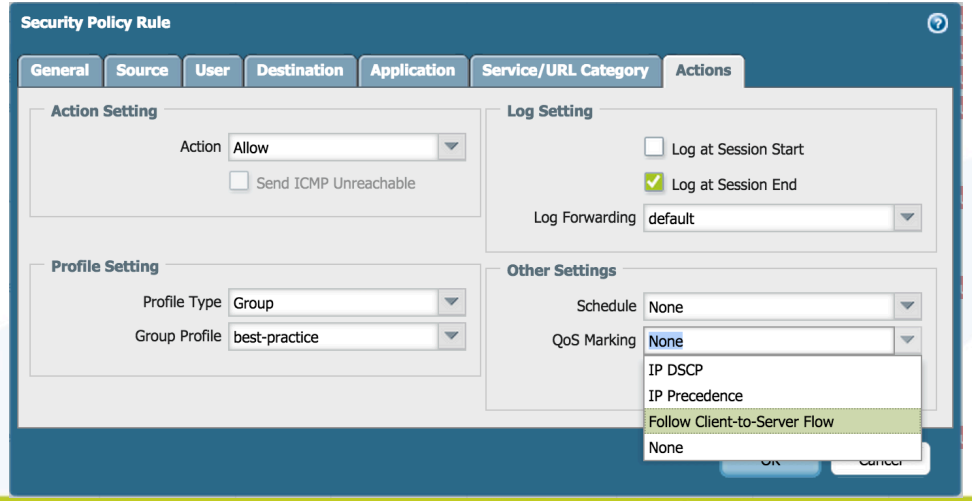
Neighbor discovery protocol proxy supporting NPTv6

- Neighbor solicitation (NS) used to find MAC of DST IPv6 host (IPv4 ARP equivalent)
- FW's neighbor advertisement responds to intercept for host behind NPTv6 rule



Session based DSCP support

- Permits shaper selection based on DSCP values for consistent QoS throughout the network
- Server to client flows can be marked with the same values as outbound client to server flows for consistent bidirectional QoS treatment
- New match criteria use DSCP/ToS values in the QoS policy
- Security policy now permits marking server to client flows based on markings found in reverse direction.



IPSec VPN enhancements

- IKEv2 support
  - Site to site VPN support improves performance/security and also enables dynamic routing with Microsoft Azure
  - Enabled with a simple mode switch along with IKEv2 specific config
    - HTTP certificate exchange
    - Cookie validation options
    - Authentication multiple – to force re-authentication periodically along with rekey
- IPv6 IPSec support
  - Enables connections to partners or remote sites with IPv6-only connectivity
  - Configuration hasn't changed from IPv4 support
  - Permits IPv4 or IPv6 traffic over IPv6 tunnels
    - Proxy IDs for both IP versions can be configured concurrently
- Operational enhancement - Refresh/restart IKE/IPSec via the web interface

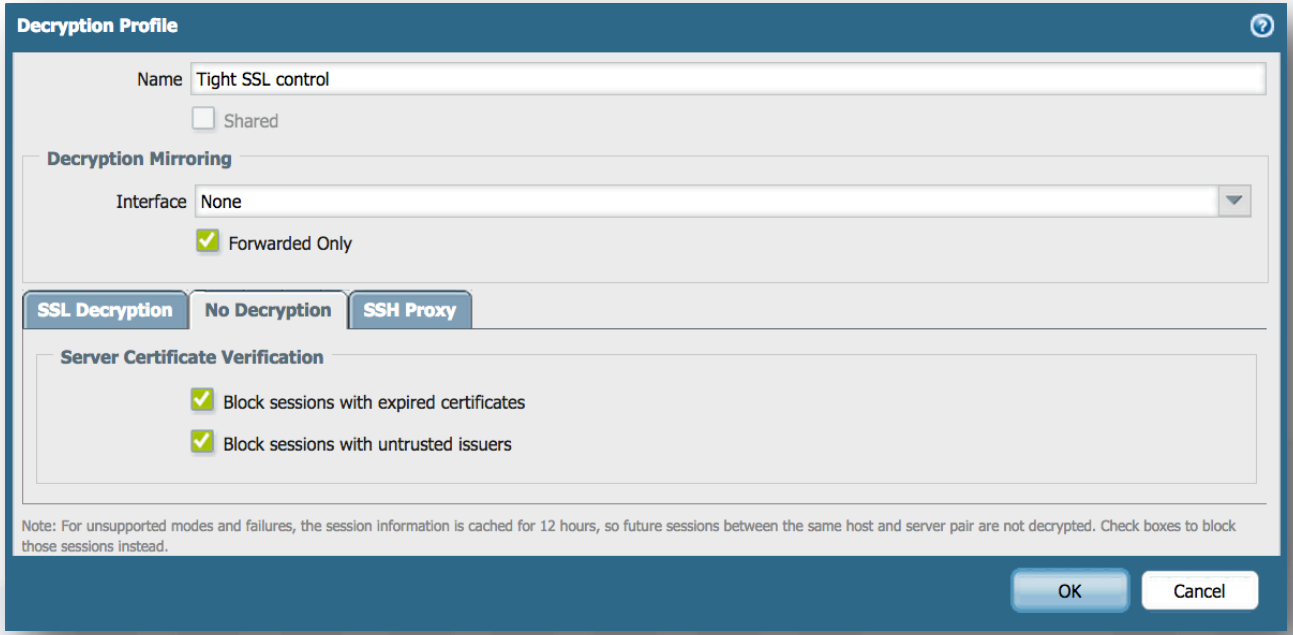
Additional PAN-OS 7.0 networking enhancements

- PA-5000 single VPN tunnel performance enhancement
  - Multiple sessions over single VPN tunnel now decrypted on multiple CPU cores
- Zone name size increase
  - Maximum name size increased from 16 to 31 bytes
- FQDN address object size increase
  - Max addresses per FQDN increased from 10 to 64 total
  - 32 IPv4 and 32 IPv6
- FW interface duplicate IP address detection
  - Support for RFC 5227 option 2
  - Detects host attempting to use firewall interface's IP address
  - Logs offending device's MAC, issues ARP to inform of proper owner
- QoS on AE interfaces
  - Now available on the PA-7050, PA-5000 Series, PA-3000 Series, PA-2000 Series, and the PA-500

SSL Decryption & Crypto

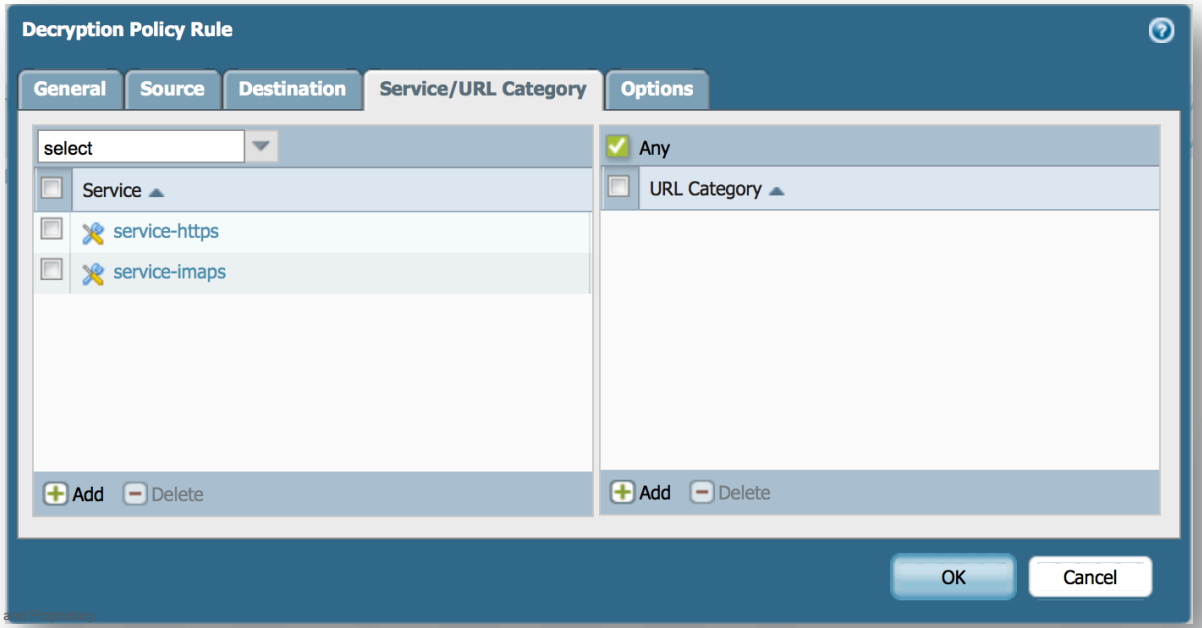
Control non-decrypted SSL traffic

- Improve user browsing behavior by controlling responses to typical certificate exceptions that can compromise security
  - Block sessions to sites with expired certificates or untrusted issuers



Decryption based on service match

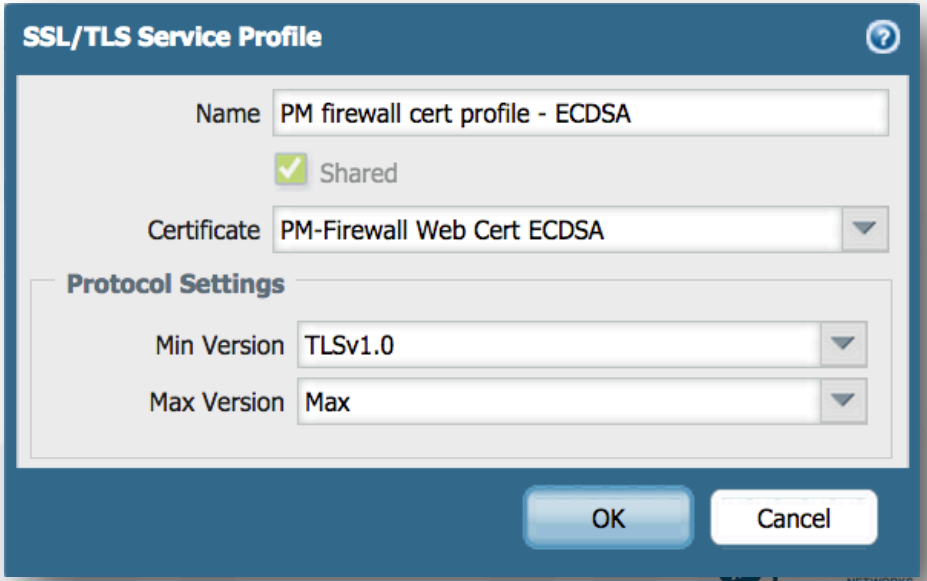
- Apply multiple inbound decryption rules to a single host to enable decryption of various services
  - E.g. Decrypt SMTP sessions and HTTPS sessions on a single host despite the use of two different certificates



SSL/TLS service profiles

- Mitigate protocol vulnerability concerns by restricting SSL/TLS protocol versions on firewall-provided layer 3 services
  - Typically encountered during PCI audits and vulnerability scans
  - E.g. BEAST, CRIME, POODLE, BREACH, etc.

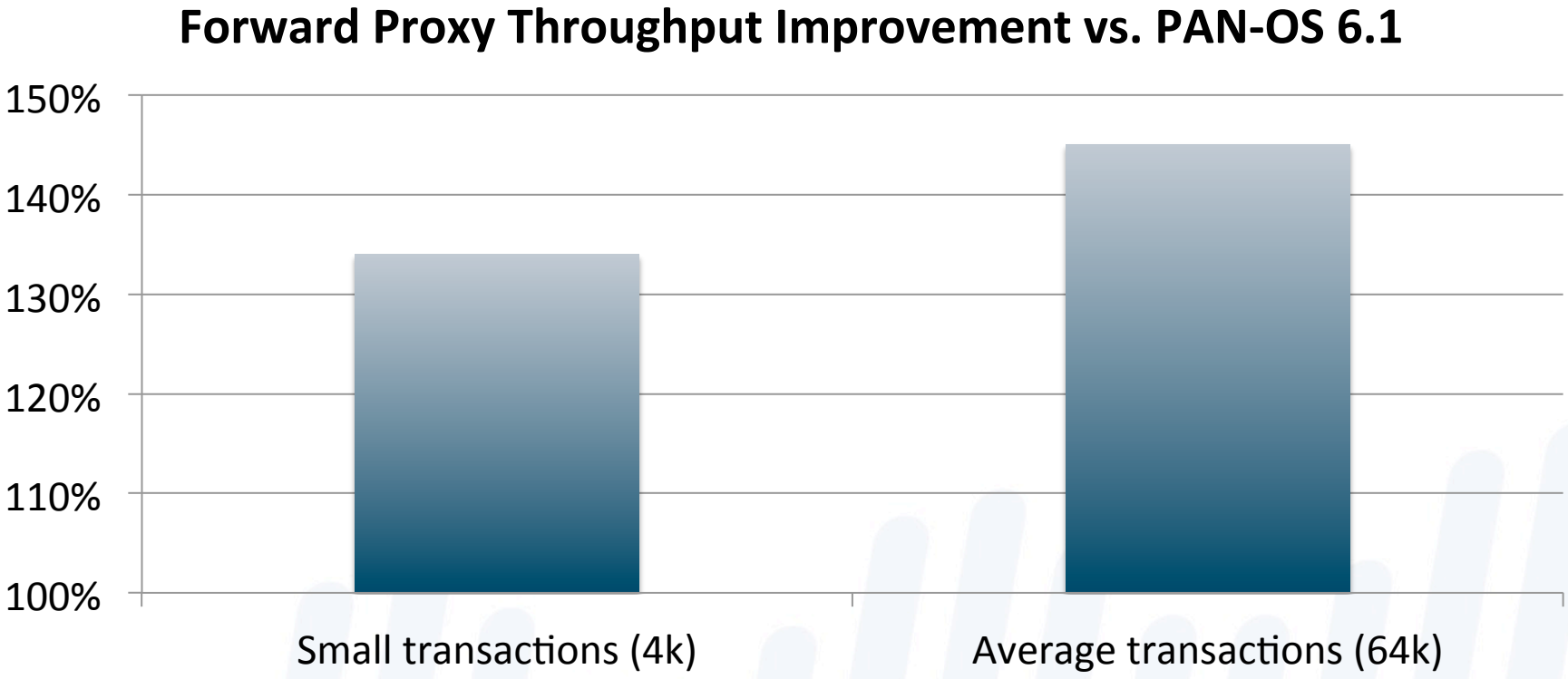
- Supported layer 3 services:
  - GlobalProtect
  - LSVPN
  - Captive portal
  - Admin web interface
  - URL override page
  - Syslog listener



Suite B cryptographic algorithm support

- Improve security with stronger Suite B compliant cryptographic algorithms
  - NIST specified algorithms sufficient to protect top secret information
- Site to site VPN – (IKE/IPSec) cryptographic algorithm additions:
  - Elliptic curve DSA (ECDSA) certificates
  - Diffie-Hellman groups 19 and 20
  - AES-GCM (128-bit and 256-bit)
- Cryptographic algorithm additions for layer 3 services provided by the firewall:
  - ECDSA certificates
  - Perfect forward secrecy (ECDHE and DHE)

SSL decryption performance improvements



SSL decryption performance improvements