# The Unknown

*Can't we really do anything to protect against it?*

*Stijn Rommens*

*Systems Engineering Manager – Northern Europe*

paloalto NETWORKS

the network security company™

# Agenda

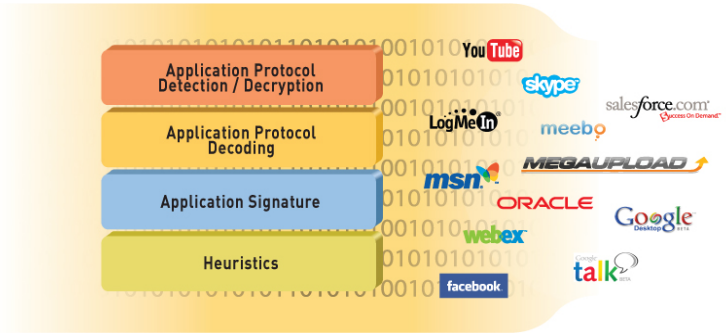
- Unknown – seen in multiple parts of your network
  - Applications
  - Users
  - Web Sites
  - Attacks
  - Malware
- Stages of Modern Malware attack cycles
- Throughout the presentation:
  - Visibility & Control with a Next Generation Network Security device

# Base Concept

# Identification Technologies Transform the Firewall

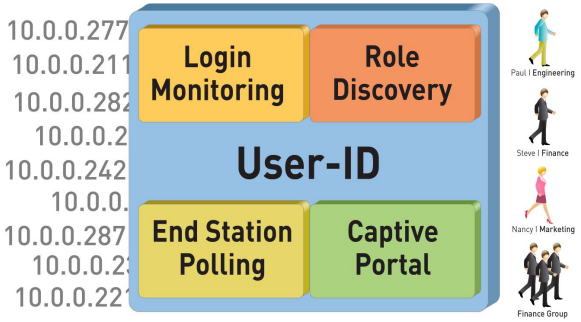
## App-ID

*Identify the application*



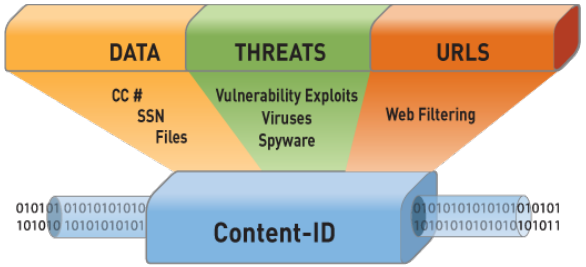

## User-ID

*Identify the user*




## Content-ID

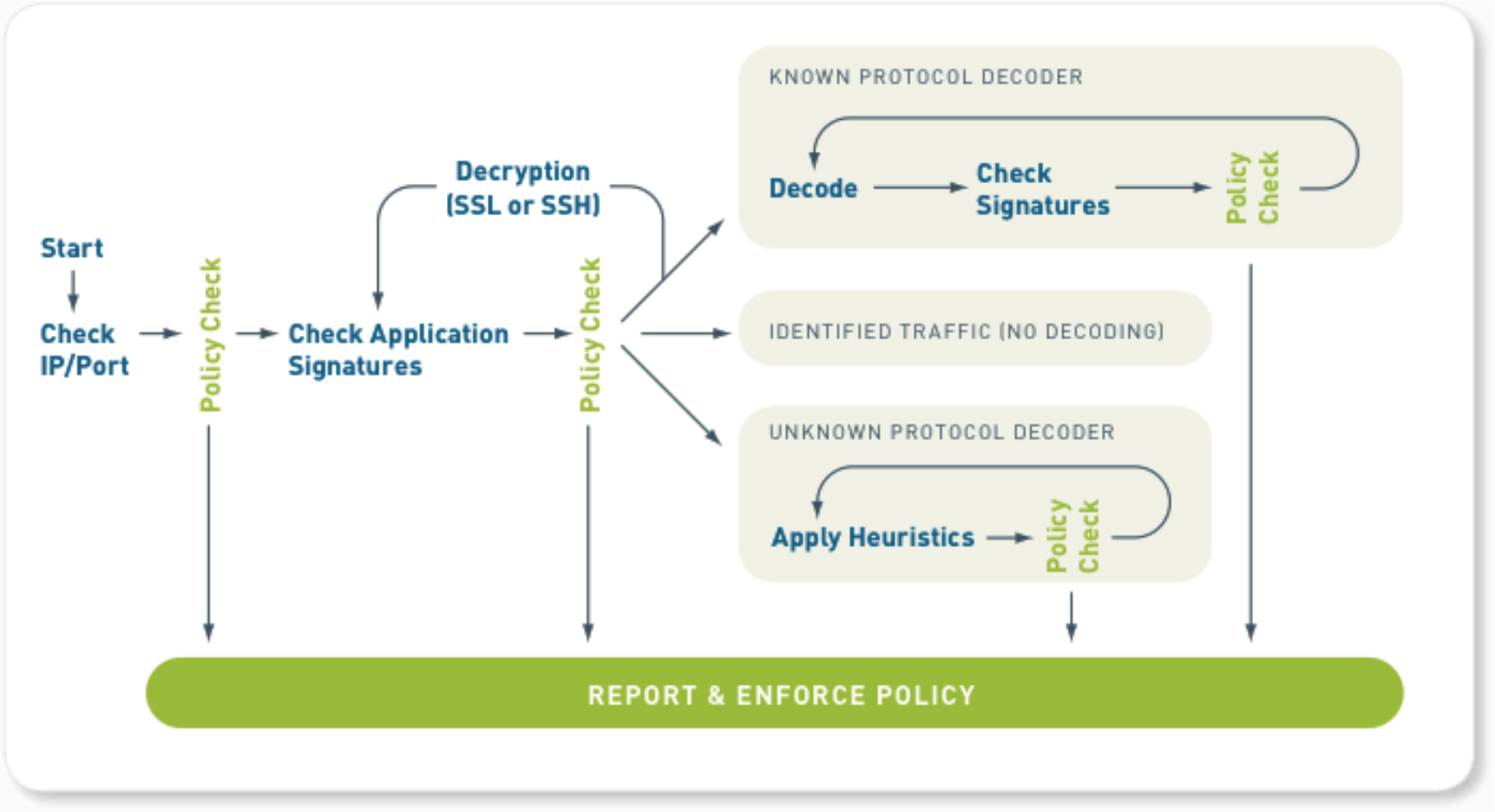
*Scan the content*



# Applications

*App-ID Features*

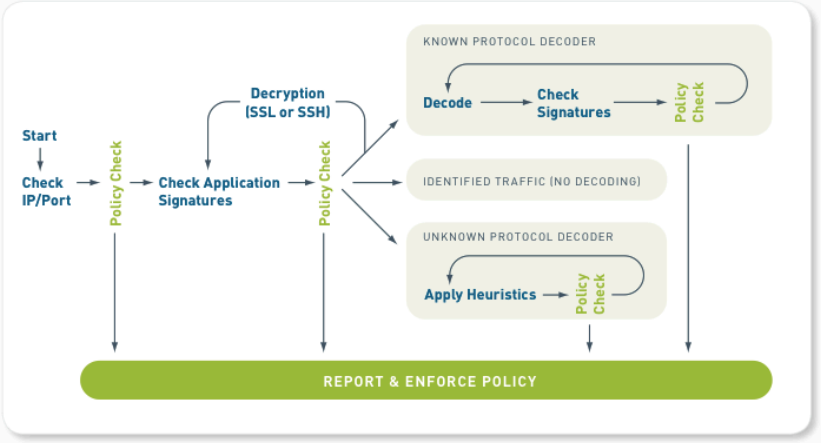
# How does App-ID work – What about Unknown




How App-ID classifies traffic

# Relevance of App-ID with Unknown Malware

- **Full stack visibility into all traffic**
  - Decodes and identifies traffic regardless of port or evasion
- **Progressive analysis**
  - Decodes tunneled protocols and communications
- **Identifies evasive techniques**
  - Encryption, proxies, anonymizers, circumventors
- **Shows non-compliant or unknown traffic**
  - Not identified by decoders, signatures or heuristics




How App-ID classifies traffic

# Custom App-ID for Unknown Traffic

- Create pattern-based signatures
  - For traffic that does not match any of our pre-defined applications

Application Research Center

apps.paloaltonetworks.com/applipedia//

APPLICATION & THREAT Research Center

paloalto NETWORKS

BLOG | APPLIPEDIA | THREAT VAULT | TOOLS | REPORTS | ABOUT

Search: facebook

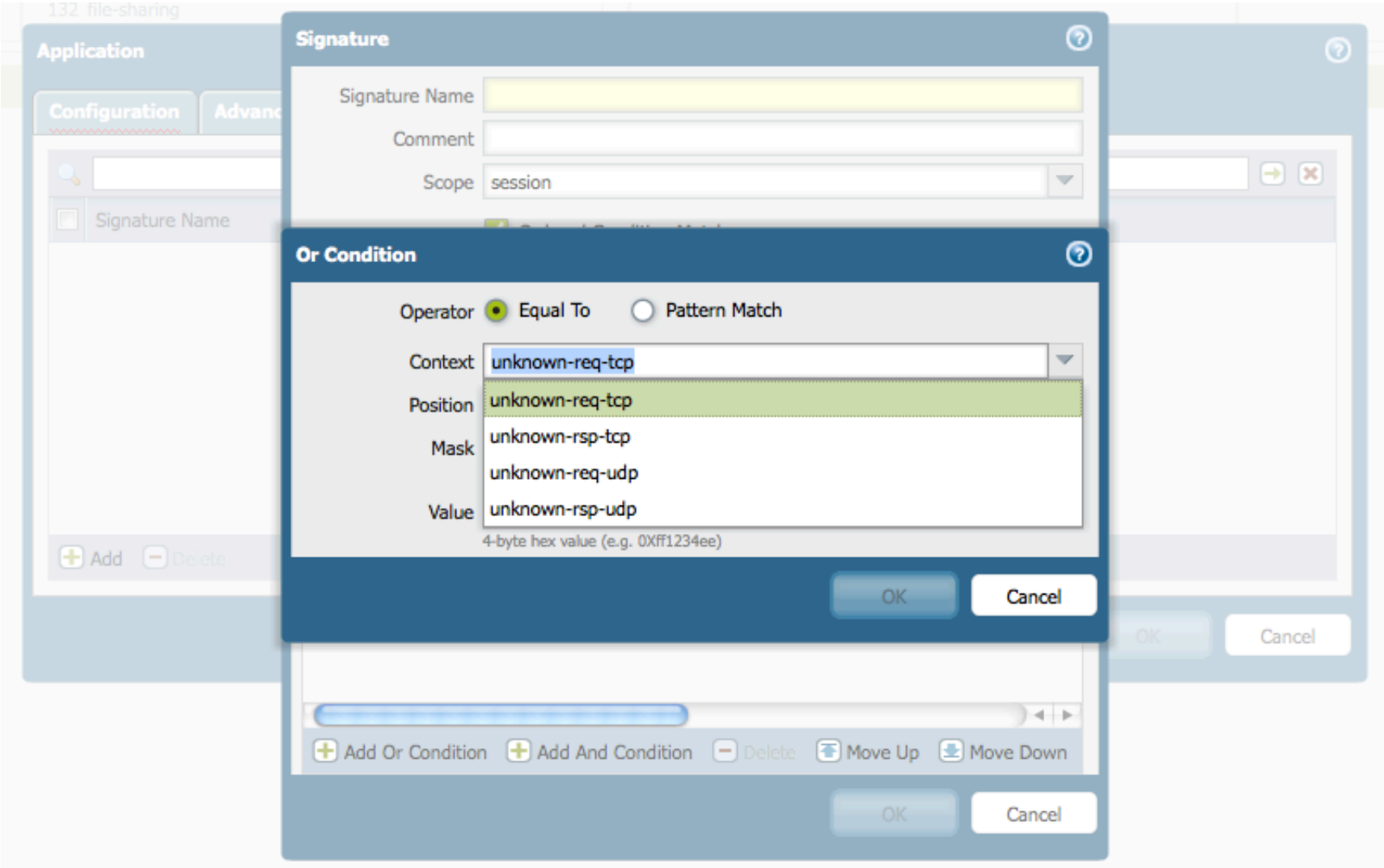
41 Applications (Clear filters)

| CATEGORY | SUBCATEGORY | TECHNOLOGY | RISK | CHARACTERISTIC |
|---|---|---|---|---|
| 1 business-systems | 4 email | 29 browser-based | 4 1 | 8 Evasive |
| 32 collaboration | 1 file-sharing | 12 client-server | 12 2 | 9 Excessive Bandwidth |
| 1 general-internet | 2 gaming | | 13 3 | 2 Prone to Misuse |
| 7 media | 8 instant-messaging | | 12 4 | 22 Transfers Files |
| | 1 office-programs | | | 5 Tunnels Other Apps |
| | 5 photo-video | | | 11 Used by Malware |
| | 18 social-networking | | | 33 Vulnerabilities |
| | 1 voip-video | | | 35 Widely Used |
| | 1 web-posting | | | |

| NAME | CATEGORY | SUBCATEGORY | RISK | TECHNOLOGY |
|---|---|---|---|---|
| facebook | | | | |
| facebook-mail | collaboration | email | 3 | browser-based |
| facebook-chat | collaboration | instant-messaging | 3 | browser-based |
| facebook-social-plugin | collaboration | social-networking | 3 | browser-based |
| facebook-base | collaboration | social-networking | 4 | browser-based |
| facebook-apps | collaboration | social-networking | 4 | browser-based |
| facebook-posting | collaboration | social-networking | 4 | browser-based |
| facebook-file-sharing | general-internet | file-sharing | 4 | browser-based |

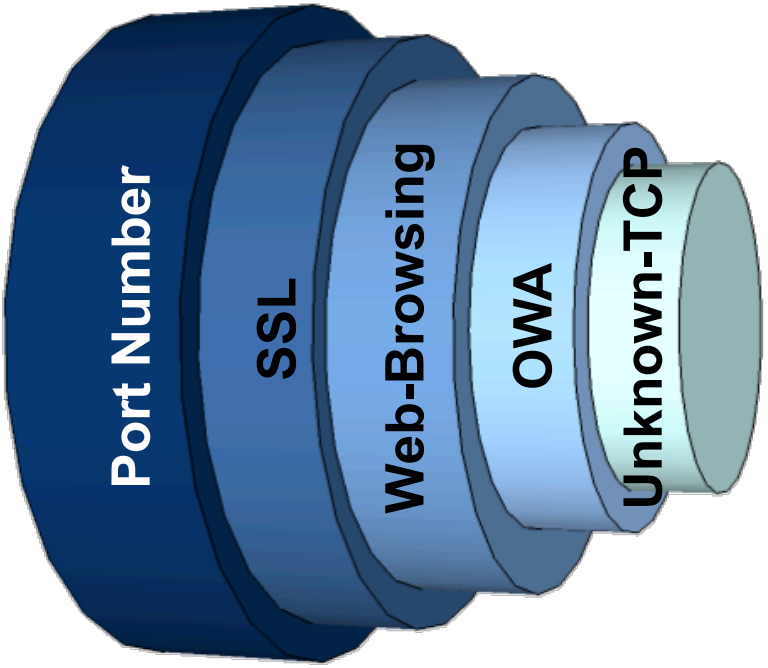
- Define App-IDs for Unknown Requests and Responses
  - For Legitimate applications -- TCP and UDP

# Custom App-ID contexts for Unknown traffic



# Palo Alto Networks App-ID

**What is the traffic and is it allowed?**
(App-ID)




**Continuous policy-driven process**
**Always the 1st task performed**
**All traffic, all ports**
**Always on**

# Users

*Any User - Known User - Specific User or Group - Unknown User*

paloalto NETWORKS

the network security company™

# User Identity

- 2 key items
  - User to IP mapping
    - *What IP did the user receive?*
    - *The mapping is required when you use identity in the policy rules*
      - Note: You can still have IP based rules as well of course
    - *The network device still sees IP addresses in the packets*
      - Mapped to a user…
  - User to Group mapping
    - *Required to build a consistent and manageable policy*
    - *Tip: Always try to avoid using individual users in a policy*

# User to IP mapping

- Preferably, this mapping is learned automatically
  - Reading out security event logs from
    - *Active Directory*
    - *Exchange Server*
  - Updating the firewall via the API, by integrating with
    - *a Wireless solution, already deployed*
      - Like Cisco, Aruba, Enterasys, ..
    - *NAC system*
    - *Simple endpoint integrated script (perl, VB, …)*
    - *Or any other solution from where users and IP addressed can be parsed from*
- Explicit authentication is possible still as an add-on
  - Via a browser (Captive Portal) or (GlobalProtect) agent

# User to Group mapping

- User to Group enumeration is an independent process
  - Identity server can be different than the user to IP mapping one
- Possible Result:
  - Users could be authenticated via AD or a certificate
  - Group mapping could occur against an open LDAP infrastructure
- Advantages:
  - Jobs/functions can be linked with a group
  - Groups can be referenced from a policy
  - Result: access to job related applications is easily maintainable

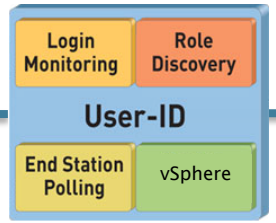
# Net value of User Awareness

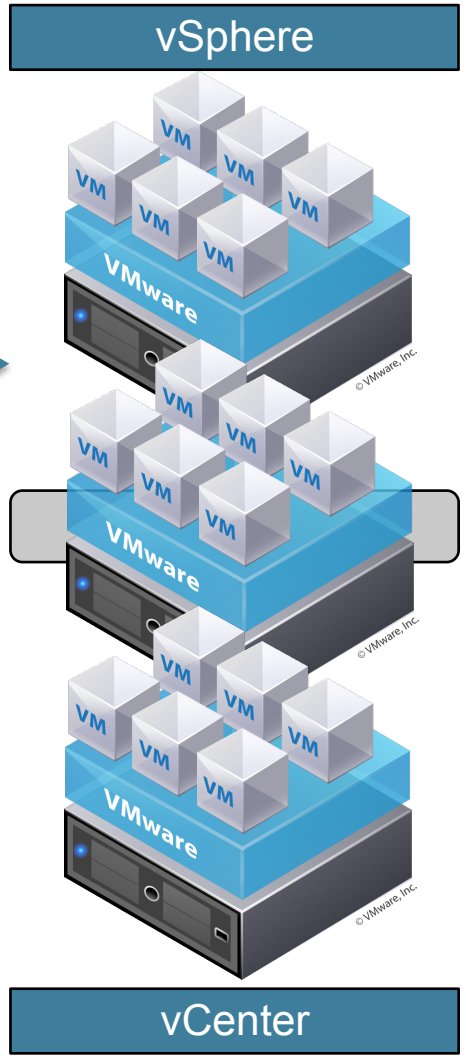
- Consistent security policies -- enterprise/organization wide
  - Users are NOT confused anymore
    - *always same workflow → both in the network as well as from remote!*
    - *Your assets are protected at all times*
- Less firewall maintenance
  - 'new' users do not need provisioning on the firewall
  - 'old' or 'leaving' users do not trigger a policy update
- Enhanced Reporting
  - Users can have multiple IPs over time, but usually only 1 user name
  - Data mining will be optimized for the same reason
- Better access control for 'unknown' users
  - Which can be tracked much easier as well

# What about systems

- Wouldn't it be great to track not only users?
- Tracking servers might be useful as well
  - Both as a source or destination in a policy
- 2 options exist:
  - Fully Qualified Domain Names
    - *When DNS results can be trusted*
    - *1 object can be resolved to multiple IP addresses*
    - *TTL is respected & FQDN objects will be refreshed (not requiring a policy push)*
  - The API when i.e. a hypervisor is used
    - *Very easy integration via scripting, which is very common in virtual environments*
    - *VM Motion with different subnets would not have any impact on accuracy*

# Use Case: VM-ID vSphere Polling




1. User-ID Agent Polls vCenter or ESX(i)
2. Agent Publishes VM Mapping
3. VM Visibility in ACC
4. Dynamic VM Adds/Moves auto-sync

**Top Sources**

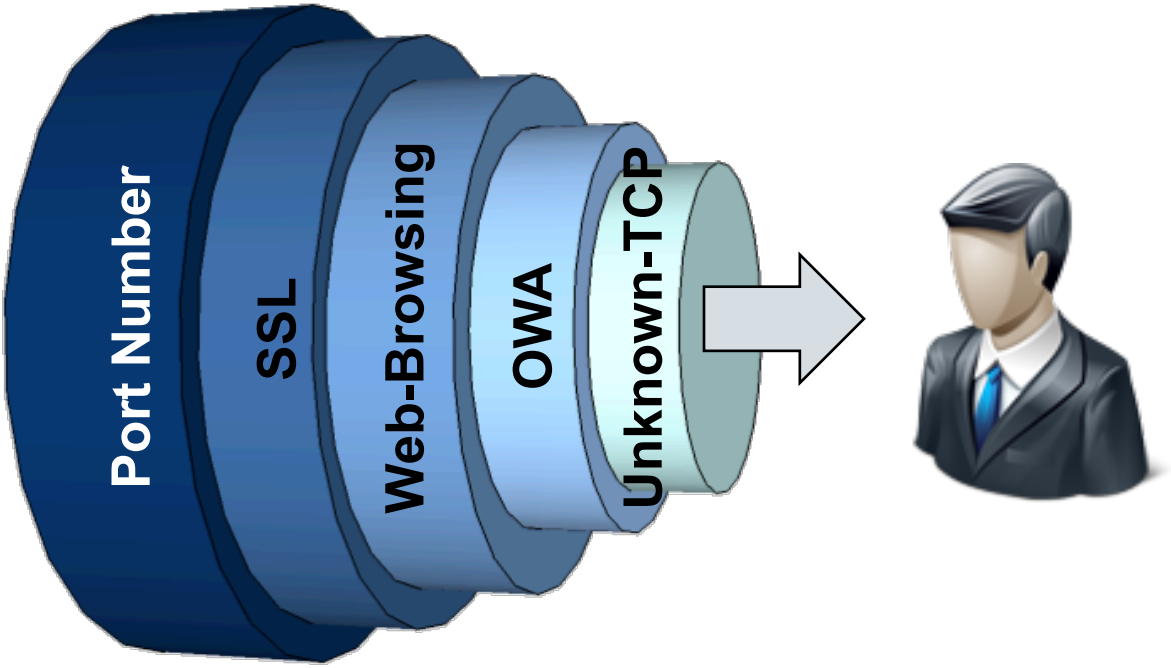
| | Source address | Source Host Name | Source User | Bytes | Sessions |
|---|---|---|---|---|---|
| 1 | 10.30.10.101 | 10.30.10.101 | win7-564d47f0-a182-7fc0-2e68-b | 1.2 M | 4.0 K |
| 2 | 10.30.10.102 | 10.30.10.102 | ubuntu-564de08b-8d30-4e3b-cadc | 639.5 K | 2.3 K |
| 3 | 10.30.10.103 | 10.30.10.103 | winxp-564db5c4-703d-c248-25bc- | 463.5 K | 1.4 K |

***Binds VM->IP***

***Report on VM and User->VM Activity***

# Palo Alto Networks integrated solution

| What is the traffic and is it allowed? (App-ID) | Allowed for this specific user or group? (User ID) |
| --- | --- |




**Continuous policy-driven process**

**Always the 1st task performed**

**All traffic, all ports**

**Always on**

# Time for some reflection

- Application Control
  - Positive enforcement of applications – NOT ports
    - *Increases security by reducing the attack surface*
- User Control
  - Allows for wider access through simplified policies
    - *IP follows the user*
    - *Users instead of IPs get access rights*
- But what about content and malware detection?
  - Let's take a step back first and review this high-level…

# Content Scanning

*The known is what we are used to scan for…*

*What about the real threat - The Unknown?*

paloalto NETWORKS

the network security company™

# Content Security

- Many different point products are in use today
  - AV
  - IPS
  - Sandbox
  - …
- Not all organization have a SIEM to correlate all together
- Let's review the 5 steps again and analyze our options…

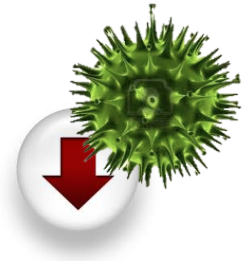
# Is it really impossible to prevent The Bait?

- The bait no longer is solely done through
  - An e-mail with an embedded malware link or file (PDF) attached
  - A post on a social media web site
- New methods arise with smartphones and tablets…
  - A QR code

# QR Codes (this one is save ;-)

- QR code
- Barcode on steroids
- Jumping-off point to the online world
- Dream to marketeers
- Now also used by cybercriminals to direct mobile phone users to malicious websites and infect them with malware

www.jump.to/xrfkjsg?exec



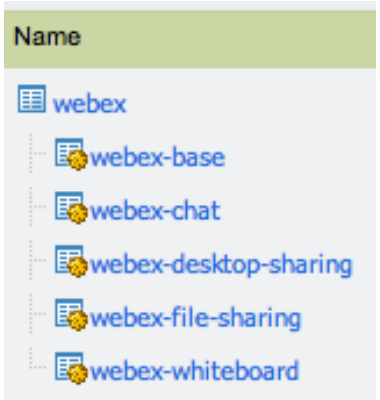
drive-by download

# How to protect your assets against this vector?

- AV solution?
  - Only if the file is recurring and has been seen in the wild before
- URL filtering solution?
  - Only if it is a fixed one and has been crawled before
- IPS solution?
  - The download is not using an exploit at all…
- Difficult, isn't it?
- Maybe a need to integrate with content-ID?
  - Control applications
  - Enforce Identity
  - Scan Content: known threats, URLs and file detection and control

# The Exploit – How to protect

- Will you only rely on an IPS
  - Limitation is that the exploit must be known to have a signature
  - Many months might pass between black-hat/white-hat detection…
- What about application awareness? – Yes, covered before...
  - Limiting the attack surface to only 'required' apps
    - *Not complete protocol stacks*
  - Limiting the application capabilities
    - *WebEx PowerPoint sharing: YES*
    - *WebEx FileSharing: NO*
  - Block unknown-tcp/udp




- Linking this with identity works even better
  - Why only require user authentication/authorization on your proxy?
    - *WebEx PowerPoint sharing: YES <u>for project leaders only</u>*

# Trojan Example: Port/Protocol Abuse

- Unknown traffic traversing the DNS port
- HTTP using non-standard ports

| To Port | Application | Action | Rule | Bytes |
|---|---|---|---|---|
| 8099 | web-browsing | allow | test | 561 |
| 23345 | web-browsing | allow | test | 401.9 K |
| 23345 | web-browsing | allow | test | 175.8 K |
| 80 | web-browsing | allow | test | 659 |
| 80 | web-browsing | allow | test | 659 |
| 80 | web-browsing | allow | test | 659 |
| 80 | web-browsing | allow | test | 659 |
| 80 | web-browsing | allow | test | 659 |
| 80 | web-browsing | allow | test | 659 |
| 80 | web-browsing | allow | test | 659 |
| 53 | unknown-udp | allow | test | 62 |
| 53 | unknown-udp | allow | test | 62 |

| e Time | Type | | | | |
|---|---|---|---|---|---|
| 14:54:36 | end | | | | |
| 14:54:24 | end | | | | |
| 14:54:23 | end | | | | |
| 14:53:43 | end | | | | |
| 14:53:43 | end | | | | |
| 14:53:43 | end | | | | |
| 14:53:43 | end | | | | |
| 14:53:42 | end | | | | |
| 14:53:42 | end | | | | |
| 14:53:42 | end | | | | |
| 14:53:39 | end | | | | |
| 14:53:39 | end | | | | |
| 14:53:38 | end | | | | |
| 14:53:38 | end | | | | |
| 14:53:38 | end | test | test | 192.168.180.1 | |
| 14:53:38 | end | test | test | 192.168.180.1 | |
| 14:53:38 | end | test | test | 192.168.180.1 | |

| To Port | Application | Action | Rule | Bytes |
|---|---|---|---|---|
| 8099 | web-browsing | allow | test | 561 |
| 23345 | web-browsing | allow | test | 401.9 K |
| 23345 | web-browsing | allow | test | 175.8 K |
| 80 | web-browsing | allow | test | 659 |
| 80 | web-browsing | allow | test | 659 |
| 80 | web-browsing | allow | test | 659 |
| 80 | web-browsing | allow | test | 659 |
| 80 | web-browsing | allow | test | 659 |
| 80 | web-browsing | allow | test | 659 |
| 80 | web-browsing | allow | test | 659 |
| 53 | unknown-udp | allow | test | 62 |
| 53 | unknown-udp | allow | test | 62 |
| 53 | unknown-udp | allow | test | 62 |
| 80 | web-browsing | allow | test | 659 |
| 53 | unknown-udp | allow | test | 62 |
| 53 | unknown-udp | allow | test | 62 |
| 53 | unknown-udp | allow | test | 62 |

# Trojan Example: Countermeasures

- Limit commonly misused protocols (HTTP, SSL, IRC, etc)
  - Allow only default ports for those
  - Note: Please don't read: 'Require a match on these ports first !'
- Block unknown traffic to port 53

| Application | Service | Action | Profile |
|---|---|---|---|
| web-browsing | application-d... | | |
| unknown-tcp | 53 tcp | | none |
| unknown-udp | 53 udp | | |
| any | any | | |

# Results after enforcing new policy controls

| To Port | Application | Action | Rule | Bytes |
|---|---|---|---|---|
| 80 | incomplete | allow | test | 184 |
| 80 | web-browsing | allow | test | 503 |
| 80 | web-browsing | allow | test | 503 |
| 80 | incomplete | allow | test | 62 |
| 80 | incomplete | allow | test | 62 |
| 80 | web-browsing | allow | test | 503 |
| 80 | web-browsing | allow | test | 503 |
| 80 | web-browsing | allow | test | 503 |
| 80 | web-browsing | allow | test | 503 |
| 80 | web-browsing | allow | test | 503 |
| 53 | unknown-udp | deny | fake dns | 62 |
| 53 | unknown-udp | deny | fake dns | 62 |
| 53 | unknown-udp | deny | fake dns | 62 |
| 80 | web-browsing | allow | test | 503 |

- HTTP is not allowed over the high ports so that the secondary payload is blocked
- Tunneling unknown traffic over port 53 is blocked

# Backdoor Download Protection

- Rely on URL filtering?
  - If the attack is targeted, good luck…
- But maybe we have some options.
- What if the download is a drive-by-download?
  - Mostly an executable file (backdoor needs to be installed)
  - Via an i-frame (not seen by the end user)
    - *Downloaded automatically by the browser*
- Control of download types is key
  - If it is an i-frame, you would not even see a block message…
  - For some file types, you might want to ask the user for confirmation
    - *In this situation, the file normally is not executed automatically, but saved by the user…*
- Scan newly seen files for unknown malware

# An example: Enterprise Phishing

- Shipping and Security are common topics for enterprise phishing
  - Fake DHL, USPS, UPS and FedEx delivery messages
  - Fake CERT notifications
- Ongoing Phishing Operations
  - Large volumes of malware – commonly in the top 3 of daily unknown malware seen in enterprises
  - Correlate new malware talking back to the same malware servers
  - Refreshed daily to avoid traditional AV signatures

***DHL-international-shipping-ID***

DHL-international-shipping notification

DHL-Express-Notification-UAN

United Parcel Service-Invoice

USPS Failed-Delivery_Notification

**US-CERT Operations Center Report**

USPS Report

MALWARE

# Phishing Analysis by WildFire

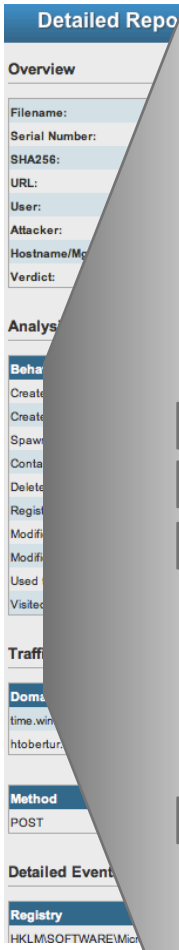
## Overview

| | | | |
|---|---|---|---|
| **Filename:** | FedEx-Shipment-Notification-Jan23-2012.exe | | |
| **Serial Number:** | 0001A100326 | | |
| **SHA256:** | 7403e9a8da93fb62d4047b724030fa4d7ad958ec0b33def7e939c6235617d681 | | |
| **URL:** | gq1.attach.mail.ymail.com/us.f1128.mail.yahoo.com/ya/secu | | |
| **User:** | unknown | **Received:** | 1/23/2012 10:59:08 AM |
| **Attacker:** | 201.216.228.109 :45952 | **Victim:** | 133.6.1.61 :25 |
| **Hostname/Mgmt. IP:** | PA-4050 | **Application:** | smtp |
| **Verdict:** | **Malware** | Virus Coverage Information | |

Analysis Summary

| Behavior |
|---|
| Created a file in the Windows folder |
| Used the POST method in HTTP |
| Created or modified files |
| Started a process from a user document folder |
| Installed a service |
| Spawned new processes |
| Listened on a specific port (backdoor behavior) |
| Deleted itself |
| Injected code into another process |
| Started or stopped a system service |

# Phishing Analysis




## Analysis Summary

| Behavior |
| --- |
| Created a file in the Windows folder |
| Used the POST method in HTTP |
| Created or modified files |
| Started a process from a user document folder |
| Installed a service |
| Spawned new processes |
| Listened on a specific port (backdoor behavior) |
| Deleted itself |
| Injected code into another process |
| Started or stopped a system service |
| Registered a file as auto-start from a local directory |
| Modified registries or system configuration to enable auto start capablity |
| Modified Windows registries |
| Changed security settings of Internet Explorer |
| Changed the proxy settings for Internet Explorer |
| Modified the network connections setting for Internet Explorer |
| Created an executable file in a user document folder |
| Visited a malware domain |
| Changed the Windows firewall policy |

# Phishing Analysis

## Detailed Report

### Overview

| | | | |
|---|---|---|---|
| Filename: | USPS report.exe | | |
| Serial Number: | 0004A100237 | | |
| SHA256: | 752271473768f43aa429bd22f67c583ff6e28c96b03278754386d49919d9aebb | | |
| URL: | unknown | | |
| User: | unknown | Received: | 12/8/2011 2:19:38 AM |
| Attacker: | 115.119.194.66 :55533 | Victim: | 134.154.183.25 :25 |
| Hostname/Mgmt. IP: | PA-2020 | Application: | smtp |
| Verdict: | Malware | Virus Coverage Information | |

### Analysis Summary

**Behavior**

Created an executable f
Created or modified fil
Spawned new proce
Contained unknow
Deleted itself
Registered a f
Modified reg
Modified V
Used th
Visite

Tr

D
tin
hto

Method
POST

Detailed Ev

Registry
HKLM\SOFTWARE\

## Traffic

| Domains |
|---|
| time.windows.com |
| htobertur.ru |

| Method | URL | User Agent |
|---|---|---|
| POST | htobertur.ru/and/image.php | Mozilla/4.0 |

# How to recognize the backchannel

- Via the IPS?
  - Possible if it is a known botnet…
  - What about unknown botnets?
- Maybe a NGFW can help if it is an unknown botnet?
  - Very likely… as it most likely will be recognized as 'unknown' traffic
- Possible actions and or methods:
  - Block unknown application traffic
  - Use heuristics to detect back channel communication
    - *Through botnet reports, checking behavior in your network*
  - C&C signatures for newly discovered malware
    - *A global sandbox can safely execute code and monitor behavior*
    - *In case of C&C traffic, appropriate action can be taken*

# Botnet Reports

**Botnet Configuration**

**HTTP Traffic**

| Event | Enable | Count | Description |
|---|---|---|---|
| Malware URL visit | ✓ | 5 | Identifies users communicating with known malware URLs based on Malware and Botnet URL filtering categories |
| Use of dynamic DNS | ✓ | 5 | Looks for dynamic DNS query traffic which could be indicative of botnet communication |
| Browsing to IP domains | ✓ | 10 | Identifies users that browse to IP domains instead of URLs |
| Browsing to recently registered domains | ✓ | 5 | Looks for traffic to domains that have been registere within the last 30 days |
| Executable files from unknown sites | ✓ | 5 | Identifies executable files downloaded from unknowr URLs |

**Unknown Applications**

| Unknown TCP | | Unknown UDP | |
|---|---|---|---|
| Sessions Per Hour | 10 [1 - 3600] | Sessions Per Hour | 10 [1 - 3600] |
| Destinations Per Hour | 10 [1 - 3600] | Destinations Per Hour | 10 [1 - 3600] |
| Minimum Bytes | 50 [1 - 200] | Minimum Bytes | 50 [1 - 200] |
| Maximum Bytes | 100 [1 - 200] | Maximum Bytes | 100 [1 - 200] |

**Other Applications**

✓ IRC

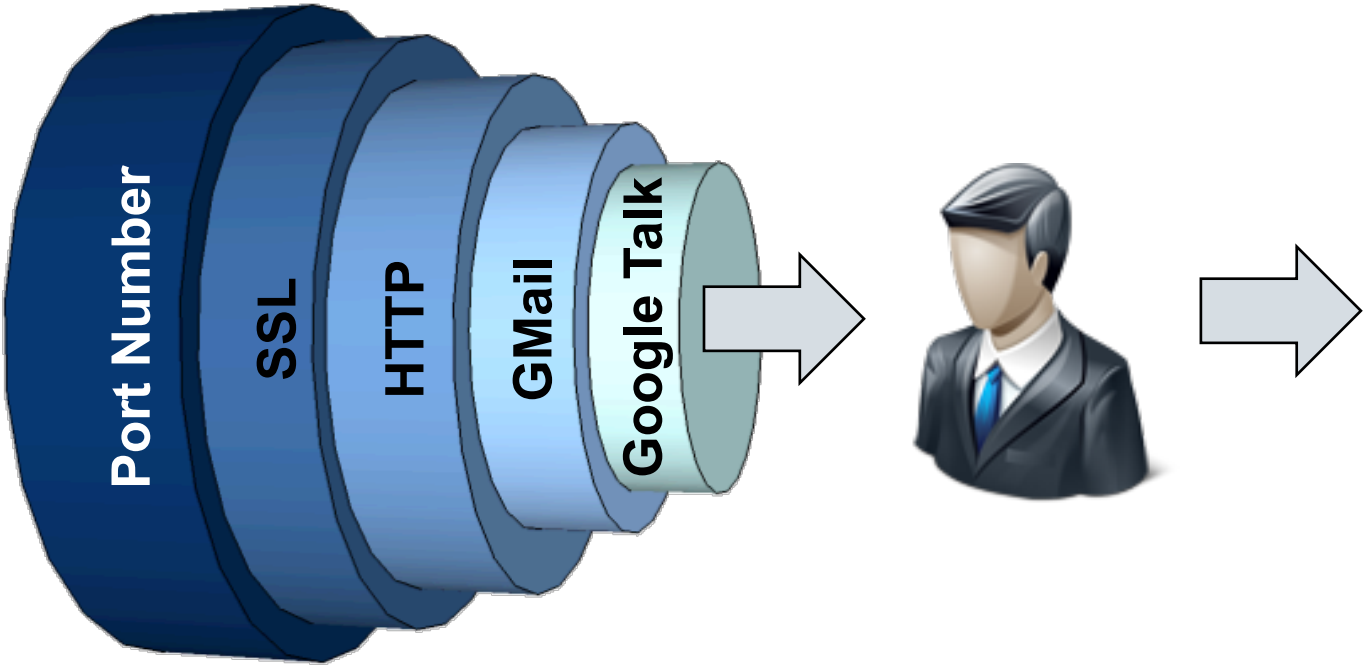
OK Cancel

# Prevent the steal

- User your AV or IPS?
  - Very doubtful…
  - The attacker
    - *Is collecting your assets, not viruses*
    - *Is not using attacks anymore, he's already in your network*
- No deep content scanning will work!!!
  - Correct network segmentation and identity control needed
    - *Limit access to crucial data to identified users*
      - The attacker now needs to target and compromise systems of specific users
        - *Targeting a random IP address won't do anymore*
    - *Implement correct network segmentation and network extension*
      - Just taking control of the right system might not be sufficient

# Palo Alto Networks integrated solution

| What is the traffic and is it allowed? (App-ID) | Allowed for this specific user or group? (User ID) | What risks or threats are in the traffic? (Content ID) |
|---|---|---|




**Continuous policy-driven process**

**Always the 1st task performed**

**All traffic, all ports**

**Always on**

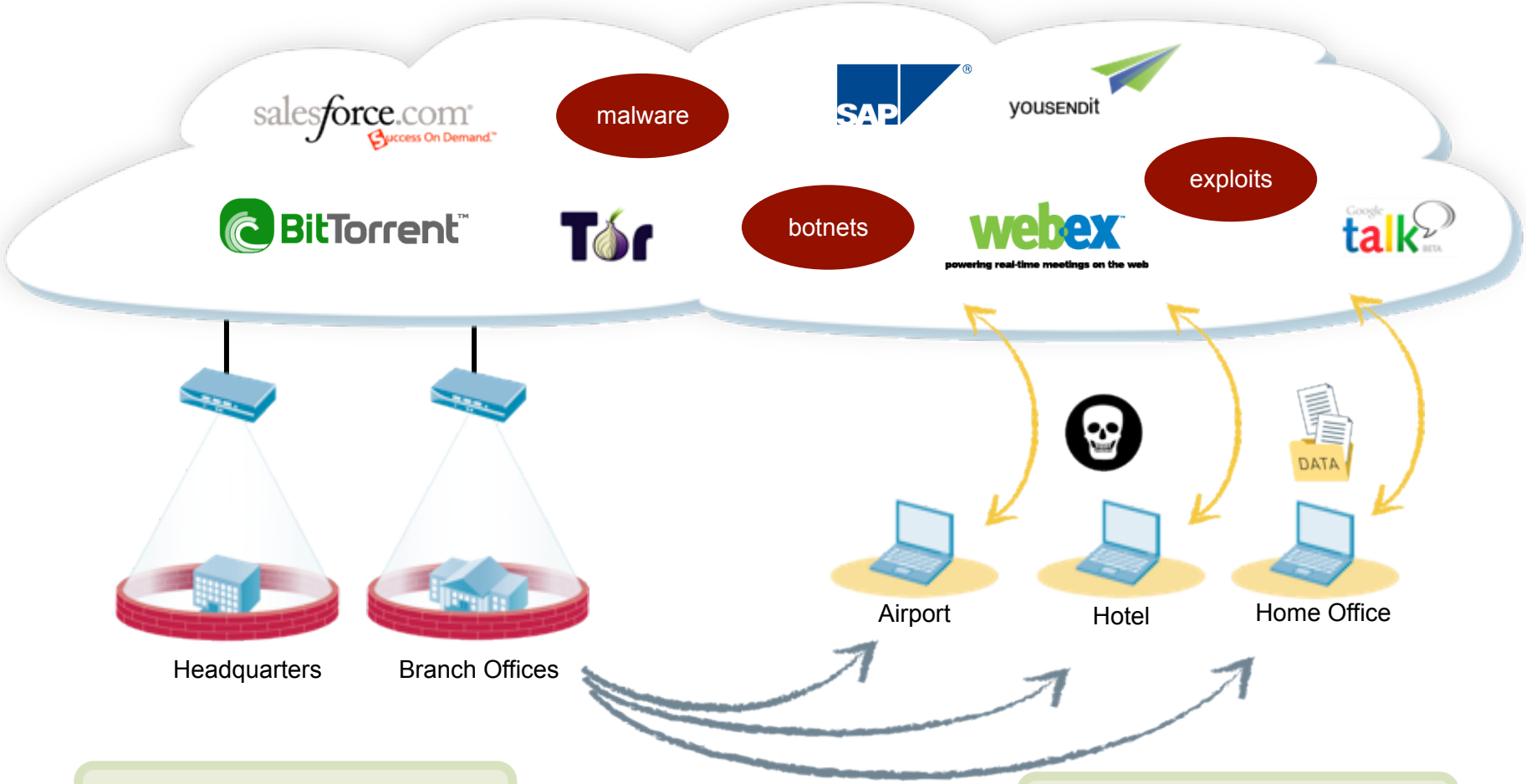
- **High block rate - known signatures**
- **13M Samples 50k per day**
- **Block malware sites**
- **Forward unknown files to a sandbox**
- **Report on network behavior and usage**

# The office building is not the perimeter anymore

paloalto NETWORKS

the network security company™

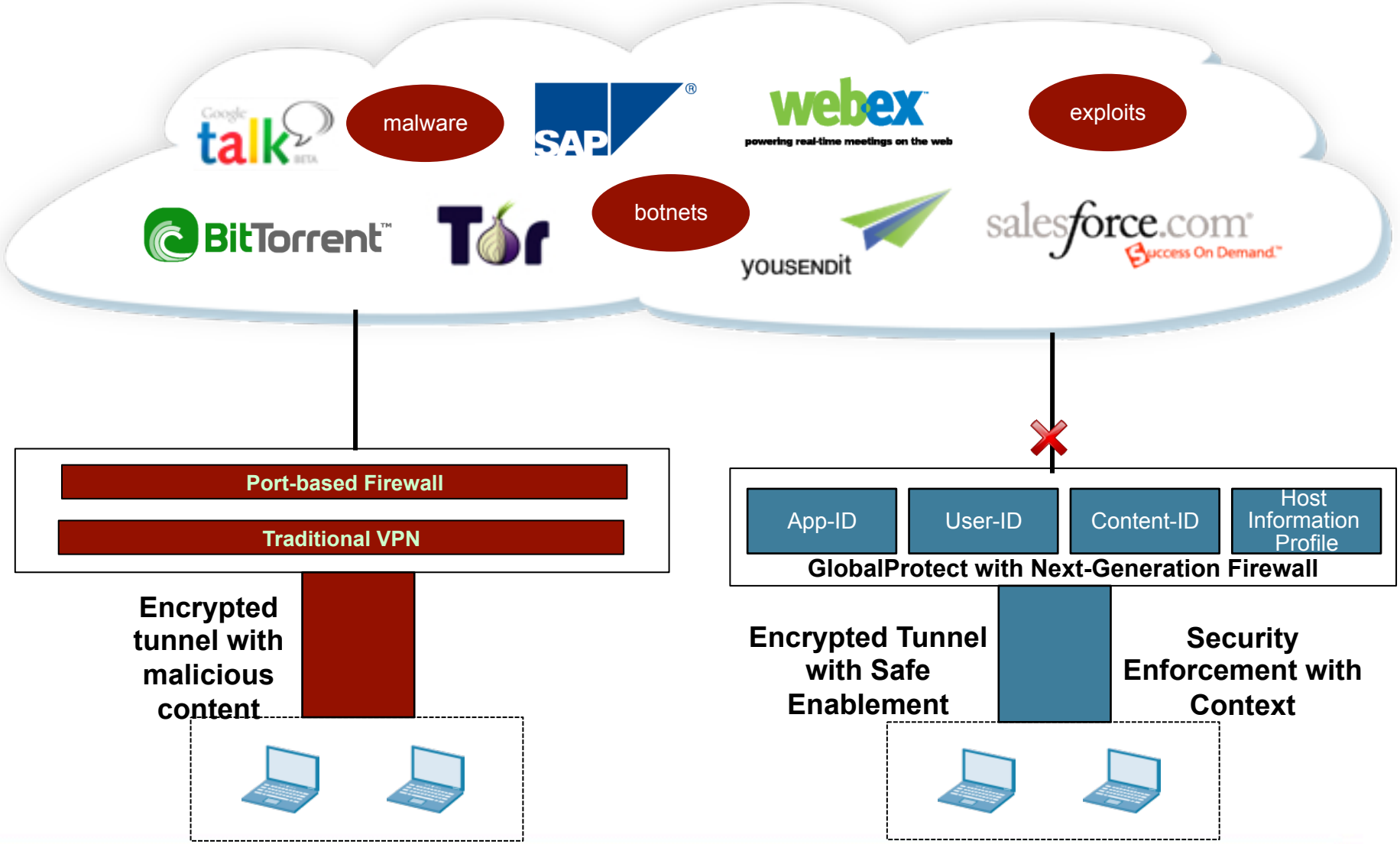
# Challenge: Quality of Security Tied to Location



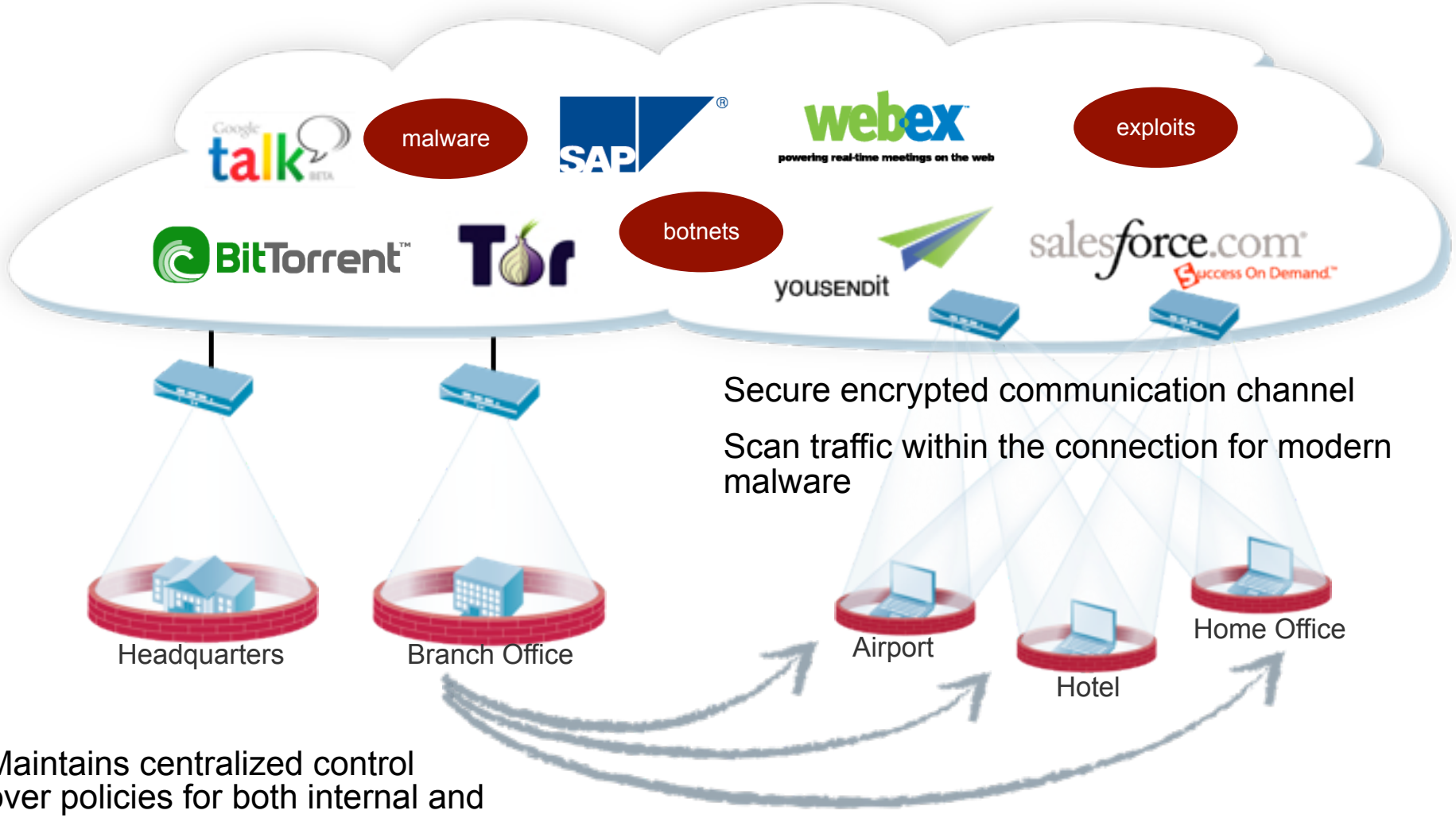

Enterprise-secured with full protection

Exposed to threats, risky apps, and data leakage

# GlobalProtect vs Remote Access VPN



# GlobalProtect: Protected Connectivity




Secure encrypted communication channel

Scan traffic within the connection for modern malware

Maintains centralized control over policies for both internal and external users

# Thank you!

paloalto NETWORKS

the network security company™