# SSL Decryption

**Mike Perez**
IT Project Manager
County of Monterey

**Jon Robinson**
President
Digital Scepter

ANAHEIM, CA | MAY 21-24, 2018

# Disclaimer

Disclaimer: No one document can be the ideal solution for every customer.
Each customer that uses this data must have an understanding of their environment to implement these Best Practices. Also, you must understand that these Best Practices are merely suggestions and can possibly disrupt normal business activity. Please implement these features with a good understanding of what you are doing before committing any of these recommendations.

# About Digital Scepter

digitalscepter

- About Digital Scepter
  - Security focus
  - Palo Alto focus, since 2007
  - No shelfware
- digitalscepter.com

# About County of Monterey

- Monterey County is a county located on the Pacific coast of the U.S. state of California. As of the 2010 census, the population was 415,057. The county seat and largest city is Salinas. Monterey County comprises the Salinas, CA Metropolitan Statistical Area. It borders the Monterey Bay, from which it derives its name. The northern half of the bay is in Santa Cruz County. Monterey County is a member of the regional governmental agency, Association of Monterey Bay Area Governments.
- County business – approximately 4,000 employees throughout 28 County departments.
- Monterey County Information Technology Department supports core network infrastructure, applications, telecommunications and systems support.

# Decryption

Why Decrypt?

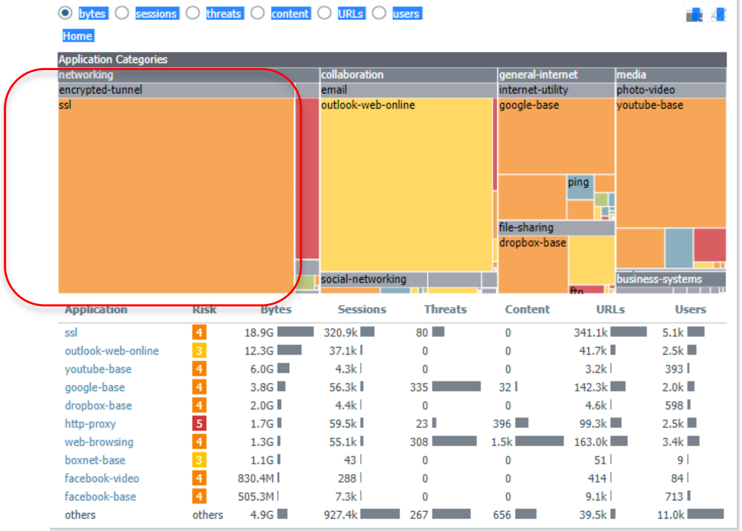
- SSL typically accounts for 40-50% of institutions overall traffic volume
- 15% of web-based, malicious Wildfire uploads are delivered via SSL

Why Monterey County decided Decrypt?

- Only http (clear text) traffic is seen by our intrusion sensors, yet more and more malware and nefarious activity is “hiding” by using https. According to our traffic statistics, nearly 60% of the county’s Internet traffic is encrypted using https, and our intrusion detection devices are currently blinded from inspecting it for command-and-control and other malicious activity.

# Decryption

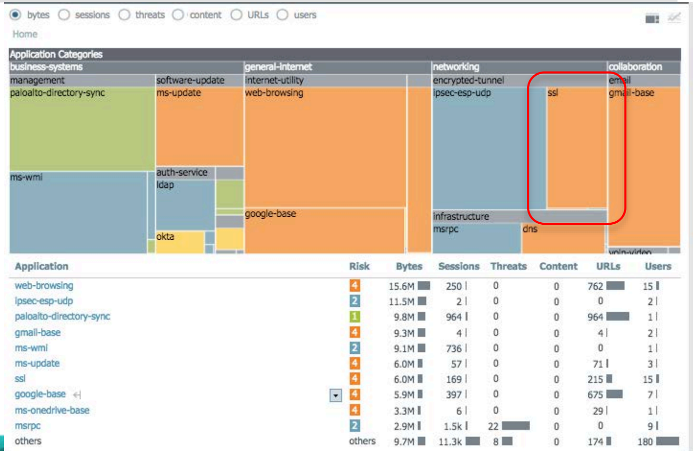
ACC Heatmap by bytes without SSL Decryption



| Application | Risk | Bytes | Sessions | Threats | Content | URLs | Users |
|---|---|---|---|---|---|---|---|
| ssl | 4 | 18.9G | 320.9k | 80 | 0 | 341.1k | 5.1k |
| outlook-web-online | 3 | 12.3G | 37.1k | 0 | 0 | 41.7k | 2.5k |
| youtube-base | 4 | 6.0G | 4.3k | 0 | 0 | 3.2k | 393 |
| google-base | 4 | 3.8G | 56.3k | 335 | 32 | 142.3k | 2.0k |
| dropbox-base | 4 | 2.0G | 4.4k | 0 | 0 | 4.6k | 598 |
| http-proxy | 5 | 1.7G | 59.5k | 23 | 396 | 99.3k | 2.5k |
| web-browsing | 4 | 1.3G | 55.1k | 308 | 1.5k | 163.0k | 3.4k |
| boxnet-base | 3 | 1.1G | 43 | 0 | 0 | 51 | 9 |
| facebook-video | 4 | 830.4M | 288 | 0 | 0 | 414 | 84 |
| facebook-base | 4 | 505.3M | 7.3k | 0 | 0 | 9.1k | 713 |
| others | others | 4.9G | 927.4k | 267 | 656 | 39.5k | 11.0k |

..and with SSL Decryption

- SSL is a smaller proportion now that we can see inside



| Application | Risk | Bytes | Sessions | Threats | Content | URLs | Users |
|---|---|---|---|---|---|---|---|
| web-browsing | 4 | 15.6M | 250 | 0 | 0 | 762 | 15 |
| ipsec-esp-udp | 2 | 11.5M | 2 | 0 | 0 | 0 | 2 |
| paloalto-directory-sync | 1 | 9.8M | 964 | 0 | 0 | 964 | 1 |
| gmail-base | 4 | 9.3M | 4 | 0 | 0 | 4 | 2 |
| ms-wmi | 2 | 9.1M | 736 | 0 | 0 | 0 | 1 |
| ms-update | 4 | 6.0M | 57 | 0 | 0 | 71 | 3 |
| ssl | 4 | 6.0M | 169 | 0 | 0 | 215 | 15 |
| google-base | 4 | 5.9M | 397 | 0 | 0 | 675 | 7 |
| ms-onedrive-base | 4 | 3.3M | 6 | 0 | 0 | 29 | 1 |
| msrpc | 2 | 2.9M | 1.5k | 22 | 0 | 0 | 9 |
| others | others | 9.7M | 11.3k | 8 | 0 | 174 | 180 |

# Decryption

## Why Decrypt?

The Decryption feature allows for inspection of SSL and SSH traffic. Below are some examples of what can be done with SSL Decryption enabled:

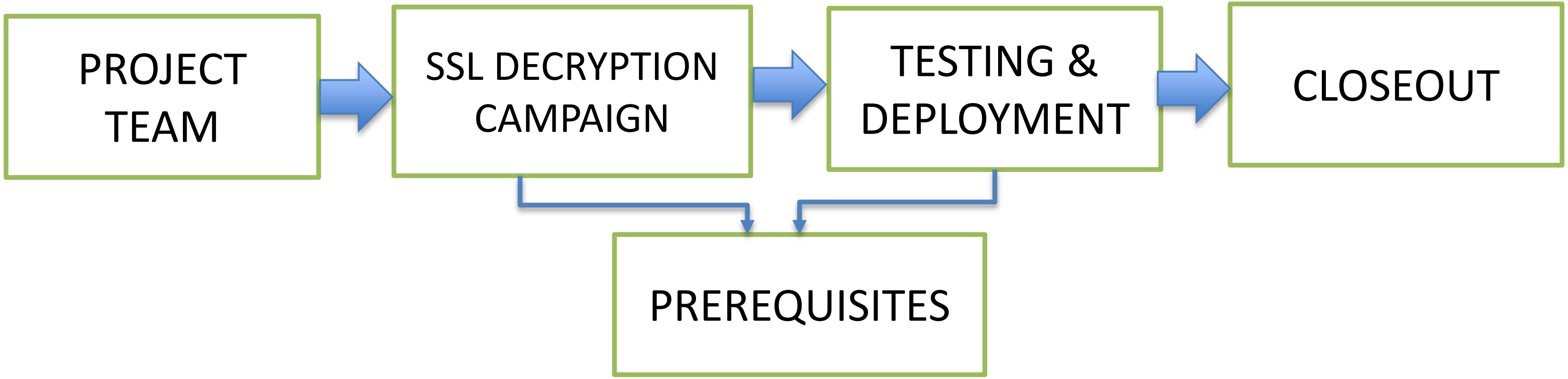
1. Identify SSL applications—e.g. logs will show application as facebook-chat instead of SSL
2. Apply Threat Prevention to encrypted traffic
3. Apply File blocking and Wildfire Analysis to files downloaded/uploaded via SSL or SSH
4. Apply URL Filtering to full URL’s, e.g. without decryption you can not selectively enable video’s on Youtube while blocking everything else. With decryption you can block youtube.com while allowing youtube.com/watch?v=2LeOH9AGJQM
5. Apply QoS to encrypted applications
6. Enforce safe search options with supported search engines

# Decryption

## Approach

1. Something is better than nothing
2. Don't let the perfect be the enemy of the good.
3. If scale is a concern, narrow the scope and focus on high risk URL categories, networks and users

# County of Monterey – SSL Project Structure



PROJECT TEAM

SSL DECRYPTION CAMPAIGN

TESTING & DEPLOYMENT

CLOSEOUT

PREREQUISITES

***GOAL – IMPLEMENT SSL DECRYPTION WITH NO IMPACT TO USERS OR COUNTY BUSINESS***

# County of Monterey – Project Team

- Project Sponsors: County CIO, Infrastructure Division Manager and ISO
- Project Manager
- IT Security Analyst
- Network Engineers
- IT Desktop Analyst
- Service Desk staff
- Department Information System Representatives
- Vendor Support

# County of Monterey – SSL Campaign

- Meeting with Department IT Staff
- Education of Staff across the County
- Email SSL Decryption information to Dept's: *Why are we decrypting traffic?*

# County of Monterey – SSL Campaign

This involves implementing industry best practices for the intentional decryption of some https (encrypted) web traffic for malware inspection purposes only.  At this time this project remains in the early testing phases but will be rolled out in limited testing sometime soon.

The intent of this project is to give our intrusion detection devices visibility into some https web traffic.  Currently, only http (clear text) traffic is seen by our sensors, yet more and more malware and nefarious activity is "hiding" by using https.  According to our traffic statistics, nearly 60% of the county's Internet traffic is encrypted using https, and our intrusion detection devices are currently blinded from inspecting it for command-and-control activity.

This implementation will provide decryption of certain https traffic on our Internet firewall for intrusion detection inspection only.  Per our vendor's best practice recommendation (and discussed at our ISO meeting), traffic in the URL categories of financial services, government, and health and medicine will NOT be decrypted in any manner. **This means that any PII or financial data in these categories will never be decrypted (and that's ok).**

From there, any traffic from high risk websites such as advertising networks, email, dynamic dns, etc. will be configured as "must decrypt".  Traffic must be decrypted for inspection by our intrusion detection sensors or it will be dropped and not delivered.

**Any other traffic is considered "best effort" (see below) and will be decrypted and inspected as much as technically possible (but will never be dropped). –*Author, Daniel Kern Information Security Officer for the County of Monterey***

# County of Monterey – Prerequisites

- Staff training on PAN – handling SSL traffic, rules, exceptions, etc. | Analyst – troubleshooting SSL related tickets.
- Service Desk – Service Now: created specific category for incoming tickets.
- What applications will not be decrypted? Office 365, specific department applications. Add these to exception list
- What certificate will be used (self-signed vs enterprise CA)
- How will the certificate be propagated through your enterprise? GPO, SCCM?
- AD structure – Security Groups that were named by dept. which included every employee – no generic accounts
- Plan for department rollout – create phase approach schedule

# *Hey there! Can I peak at your traffic?* ☺
# Testing of SSL Decryption

**Test #1 – IT Dept.**

Step 1 - IT Managers

Step 2 – 5 staff members from different groups

Step 3 – 15 additional staff members

Objectives:
What were the pain-points?
User experience?

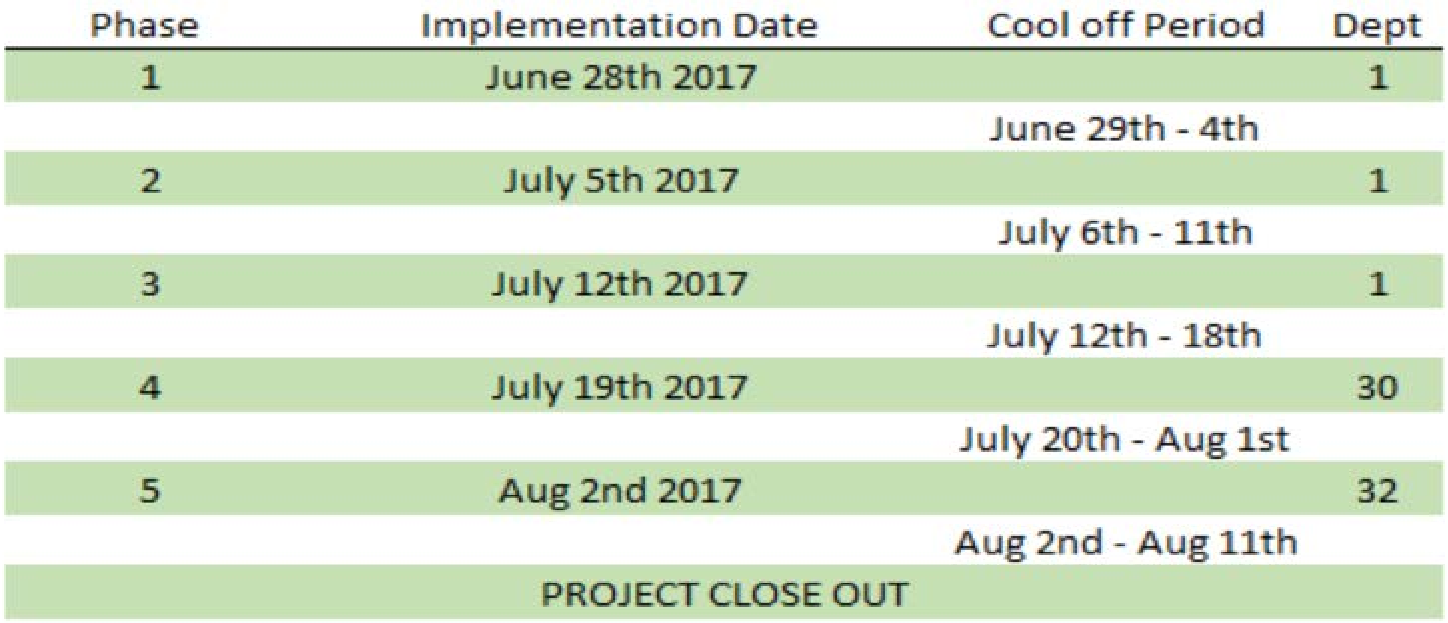
**Test #2 – County Depts.**

Step 1 – 5 staff member from 5 different dept.

Ranging from hot to cold departments

Objective: This is SSL Decryption – how does it feel?

# County of Monterey – Implementation



| Phase | Implementation Date | Cool off Period | Dept |
|---|---|---|---|
| 1 | June 28th 2017 | | 1 |
| | | June 29th - 4th | |
| 2 | July 5th 2017 | | 1 |
| | | July 6th - 11th | |
| 3 | July 12th 2017 | | 1 |
| | | July 12th - 18th | |
| 4 | July 19th 2017 | | 30 |
| | | July 20th - Aug 1st | |
| 5 | Aug 2nd 2017 | | 32 |
| | | Aug 2nd - Aug 11th | |
| PROJECT CLOSE OUT | | | |

# Decryption

## So, How Does Decrypt Work?

- Your Palo Alto Networks firewall acts as an SSL forward proxy

- SSL Requests that hit the firewall and match a decryption policy are proxied

- An example:

1. An endpoint attempts to access https://www.facebook.com
2. The firewall presents the endpoint with a *.facebook.com certificate that it issues itself and the endpoint builds an SSL connection with the firewall.
3. The firewall then builds an SSL connection to https://www.facebook.com on that endpoints behalf
4. The one SSL session between the endpoint and Facebook effectively becomes two, endpoint to firewall and firewall to Facebook
5. This allows the firewall to see the unencrypted traffic and is otherwise known as a "Man in the Middle" attack.

# Decryption

## Legal Concerns

- There normally isn't an expectation of privacy on government networks
- Explain the project to your legal counsel and get their opinion

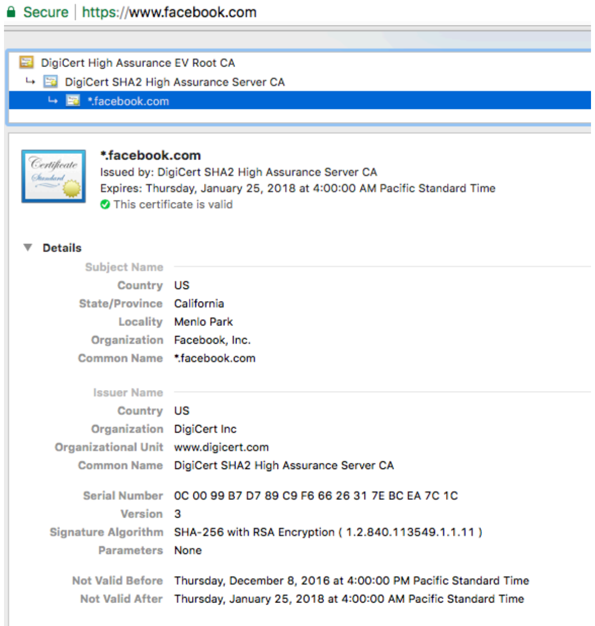
In the case of County of Monterey, the ISO worked with the departments counsel.  Below is a summary of her opinion:

*I understand that decrypted web traffic is inspected by security tools for malware; the decrypted information is not stored or kept in any way or evaluated by a human being who might thereby be inappropriately privy to personal or legally protected, private information.*

*I am comfortable with this scenario and don't see any obvious legal risks posed by it.*

# Decryption

## Not Decrypted



Secure | https://www.facebook.com

DigiCert High Assurance EV Root CA
↳ DigiCert SHA2 High Assurance Server CA
↳ *.facebook.com

***.facebook.com**
Issued by: DigiCert SHA2 High Assurance Server CA
Expires: Thursday, January 25, 2018 at 4:00:00 AM Pacific Standard Time
✓ This certificate is valid

▼ **Details**

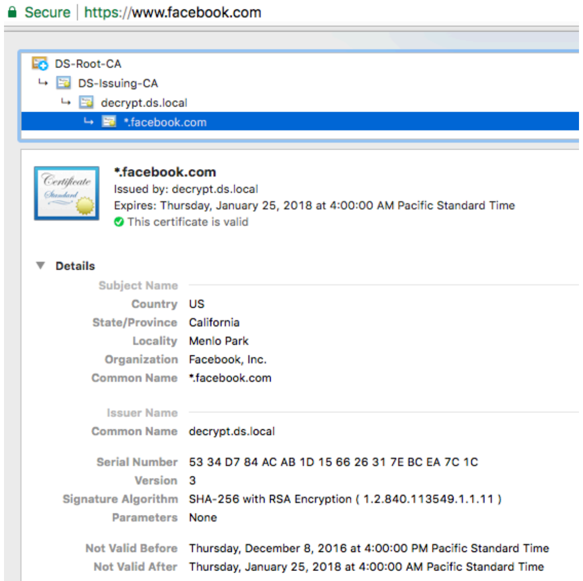
Subject Name
Country US
State/Province California
Locality Menlo Park
Organization Facebook, Inc.
Common Name *.facebook.com

Issuer Name
Country US
Organization DigiCert Inc
Organizational Unit www.digicert.com
Common Name DigiCert SHA2 High Assurance Server CA

Serial Number 0C 00 99 B7 D7 89 C9 F6 66 26 31 7E BC EA 7C 1C
Version 3
Signature Algorithm SHA-256 with RSA Encryption ( 1.2.840.113549.1.1.11 )
Parameters None

Not Valid Before Thursday, December 8, 2016 at 4:00:00 PM Pacific Standard Time
Not Valid After Thursday, January 25, 2018 at 4:00:00 AM Pacific Standard Time

## Decrypted



Secure | https://www.facebook.com

DS-Root-CA
↳ DS-Issuing-CA
↳ decrypt.ds.local
↳ *.facebook.com

***.facebook.com**
Issued by: decrypt.ds.local
Expires: Thursday, January 25, 2018 at 4:00:00 AM Pacific Standard Time
✓ This certificate is valid

▼ **Details**

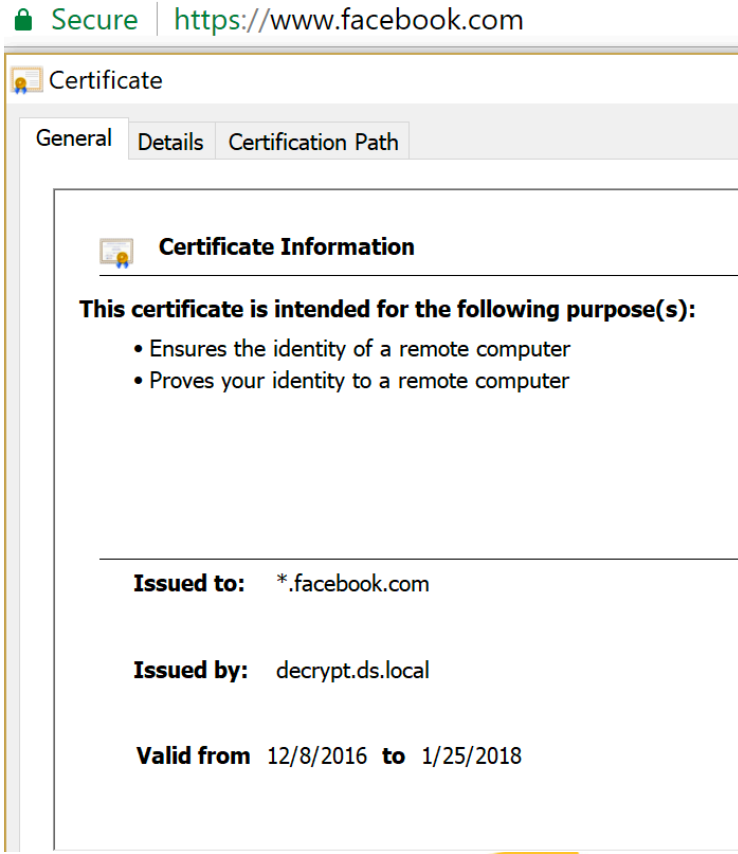
Subject Name
Country US
State/Province California
Locality Menlo Park
Organization Facebook, Inc.
Common Name *.facebook.com

Issuer Name
Common Name decrypt.ds.local

Serial Number 53 34 D7 84 AC AB 1D 15 66 26 31 7E BC EA 7C 1C
Version 3
Signature Algorithm SHA-256 with RSA Encryption ( 1.2.840.113549.1.1.11 )
Parameters None

Not Valid Before Thursday, December 8, 2016 at 4:00:00 PM Pacific Standard Time
Not Valid After Thursday, January 25, 2018 at 4:00:00 AM Pacific Standard Time

# Decryption



Secure | https://www.facebook.com

Certificate

General | Details | Certification Path

**Certificate Information**

**This certificate is intended for the following purpose(s):**

- Ensures the identity of a remote computer
- Proves your identity to a remote computer

**Issued to:** *.facebook.com

**Issued by:** decrypt.ds.local

**Valid from** 12/8/2016 **to** 1/25/2018

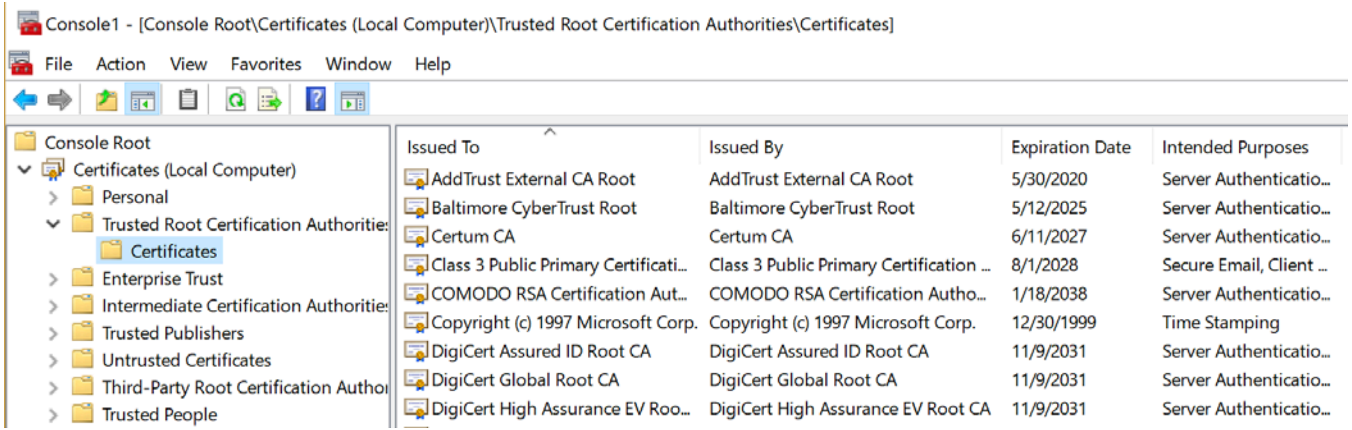
<u>Wait, How Does the Firewall Have a *.facebook.com Certificate?</u>

- Your firewall is able to build certificates on the fly to impersonate the different sites that are being decrypted
- This is done leveraging a Certificate Authority that exists on the Palo Alto Networks firewall
- Ok great, so I can order this certificate through GoDaddy,
  Comodo, or any other trusted public Certificate Authority? <u>No.</u>

# Decryption

Certificate Authority

- A Certificate Authority is responsible for issuing digital certificates.
- A common type of digital certificate is an SSL certificate, which is used to validate the identity of a website
- Your endpoint and/or browser has a list of certificate authorities that it inherently trusts



Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

- Console Root
  - Certificates (Local Computer)
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Author
    - Trusted People

| Issued To | Issued By | Expiration Date | Intended Purposes |
|---|---|---|---|
| AddTrust External CA Root | AddTrust External CA Root | 5/30/2020 | Server Authenticatio... |
| Baltimore CyberTrust Root | Baltimore CyberTrust Root | 5/12/2025 | Server Authenticatio... |
| Certum CA | Certum CA | 6/11/2027 | Server Authenticatio... |
| Class 3 Public Primary Certificati... | Class 3 Public Primary Certification ... | 8/1/2028 | Secure Email, Client ... |
| COMODO RSA Certification Aut... | COMODO RSA Certification Autho... | 1/18/2038 | Server Authenticatio... |
| Copyright (c) 1997 Microsoft Corp. | Copyright (c) 1997 Microsoft Corp. | 12/30/1999 | Time Stamping |
| DigiCert Assured ID Root CA | DigiCert Assured ID Root CA | 11/9/2031 | Server Authenticatio... |
| DigiCert Global Root CA | DigiCert Global Root CA | 11/9/2031 | Server Authenticatio... |
| DigiCert High Assurance EV Roo... | DigiCert High Assurance EV Root CA | 11/9/2031 | Server Authenticatio... |

# Decryption

How Can My Firewall Be a Certificate Authority

1. Option 1 - Leverage your corporate Certificate Authority to issue an Intermediate Certificate Authority certificate to your Palo Alto Networks firewall

2. Option 2 - Generate a self-signed Certificate Authority certificate on the Palo Alto Networks firewall

# Decryption

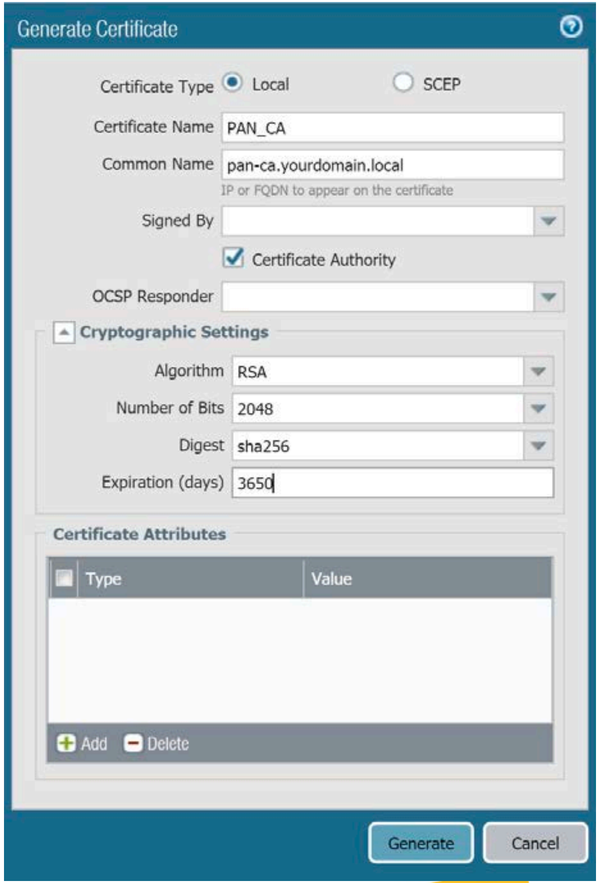
Option 1 - Intermediate CA Signed by Corporate CA

- Pros
  - Simple certificate revocation if intermediate CA is compromised
  - Since corporate CA is already trusted, no need to push intermediate CA to endpoints
- Cons
  - Requires management of corporate CA

# Decryption

Option 2 - Self-Signed Certificate Authority

- Pros
  - Doesn’t require corporate CA
- Cons
  - Less secure, no ability to revoke compromised CA
  - Requires distribution of certificate to endpoints



Generate Certificate

Certificate Type ● Local ○ SCEP

Certificate Name PAN_CA

Common Name pan-ca.yourdomain.local

IP or FQDN to appear on the certificate

Signed By

☑ Certificate Authority

OCSP Responder

Cryptographic Settings

Algorithm RSA

Number of Bits 2048

Digest sha256

Expiration (days) 3650

Certificate Attributes

| □ | Type | Value |
|---|---|---|

# Decryption

Digital Scepter Recommends Option 1

- Although we recommend option 1, it comes with the burden of understanding the risks involved with deploying and managing a private Certificate Authority
- As a best practice, we recommend deploying a two-tier Certificate Authority where you have a non-domain-joined, offline Root CA, and a domain joined, Intermediate CA.

References

- https://windowsmasher.wordpress.com/2013/03/03/single-vs-two-tier-pki/
- https://www.globalsign.com/en/ssl-information-center/what-are-certification-authorities-trust-hierarchies/

# Decryption

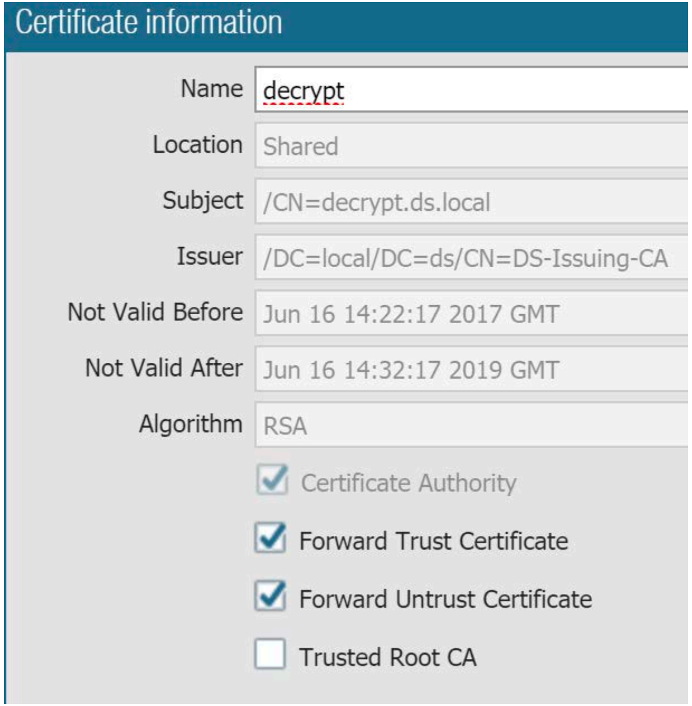
We Have Our CA, Now How Is Decrypt Enabled?

1. Whether a self signed certificate or a privately signed certificate was used, we need to assign that certificate two roles:

    1. **Forward Trust Certificate** - a trusted certificate is presented to the endpoint when the firewall is able to successfully validate the site the endpoint is connecting to

    2. **Forward Untrust Certificate** - an untrusted certificate is presented to the endpoint when the firewall is unable to validate the site the endpoint is connecting to, e.g. the certificate is expired or otherwise invalid

2. Now we need to create our Decryption policies…



Certificate information

| | |
|---|---|
| Name | decrypt |
| Location | Shared |
| Subject | /CN=decrypt.ds.local |
| Issuer | /DC=local/DC=ds/CN=DS-Issuing-CA |
| Not Valid Before | Jun 16 14:22:17 2017 GMT |
| Not Valid After | Jun 16 14:32:17 2019 GMT |
| Algorithm | RSA |

☑ Certificate Authority

☑ Forward Trust Certificate

☑ Forward Untrust Certificate

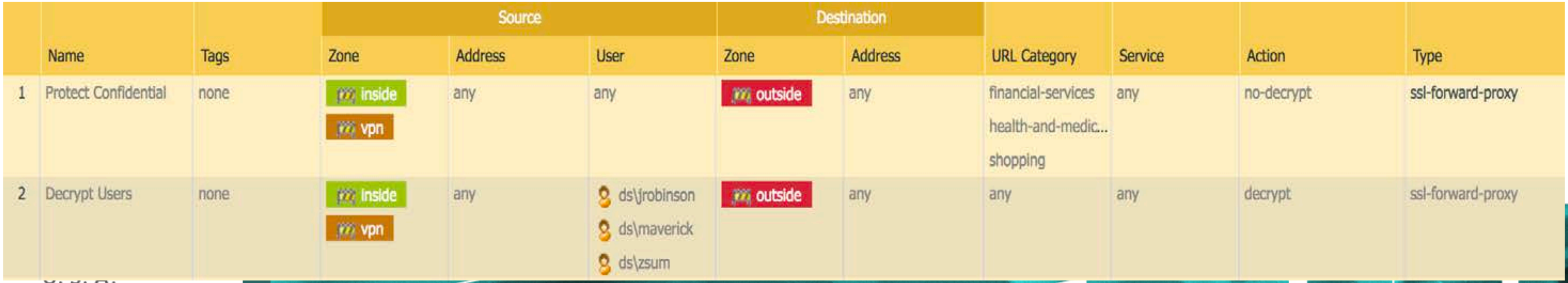
□ Trusted Root CA

# Decryption

Policies > Decryption

1. Policy 1 - A no-decrypt rule that protects URL categories that contain private data from being decrypted:
    1. **financial-services** - online banking account information
    2. **health-and-medicine** - doctor office web portals, medical records
    3. **shopping** - credit card transactions

2. Policy 2 - A general decrypt rule that decrypts all other URL categories not specified in policy 1. This can further be limited by Source and Destination user/zone/IP address

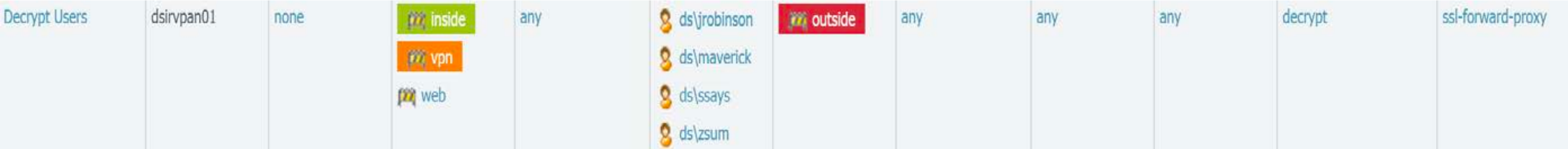


| | | | Source | | | Destination | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Name | Tags | Zone | Address | User | Zone | Address | URL Category | Service | Action | Type |
| 1 | Protect Confidential | none | inside<br>vpn | any | any | outside | any | financial-services<br>health-and-medic...<br>shopping | any | no-decrypt | ssl-forward-proxy |
| 2 | Decrypt Users | none | inside<br>vpn | any | ds\jrobinson<br>ds\maverick<br>ds\zsum | outside | any | any | any | decrypt | ssl-forward-proxy |

# Decryption

Strategy for Decryption Rollout

1. Start with a small group of users who are subject to decryption policies. Every organization will run into applications that do not support SSL Decryption. The idea is to identify these applications and create decryption exclusion policies without impact across the organization



| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Decrypt Users | dsirvpan01 | none | inside<br>vpn<br>web | any | ds\jrobinson<br>ds\maverick<br>ds\ssays<br>ds\zsum | outside | any | any | any | decrypt | ssl-forward-proxy |

2. Once the small group of users is no longer experiencing issues, expand the test group by including additional users. Consider adding an additional department/site to the decryption rule

3. Repeat the process of identifying and creating exclusions. Once you can expand the test group without affecting SSL applications, it can be enabled globally across the organization

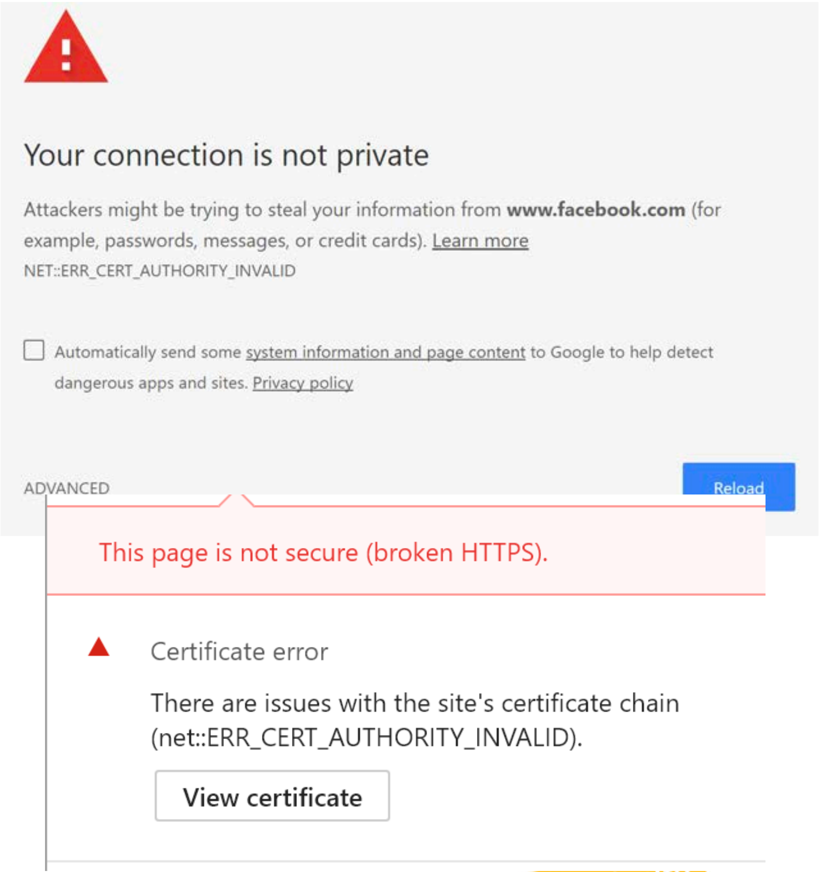
# Decryption

<u>Problem - Certificate Errors!!!</u>

- A common problem is that users receive a certificate error when being decrypted. The Chrome browser is great for troubleshooting these.

1. In Chrome, press F12 and go to **Security** tab

2. Note the error shows an invalid Certificate Authority



Your connection is not private

Attackers might be trying to steal your information from **www.facebook.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

☐ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

This page is not secure (broken HTTPS).

Certificate error

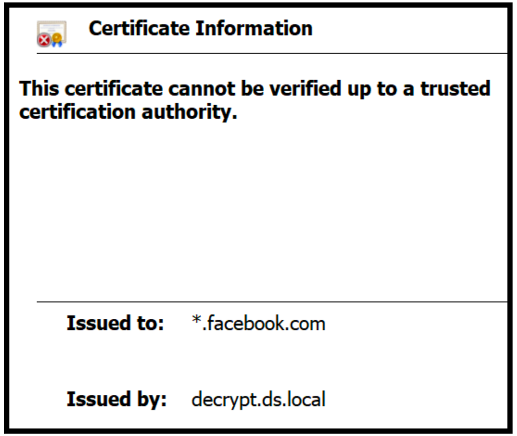
There are issues with the site's certificate chain (net::ERR_CERT_AUTHORITY_INVALID).

# Decryption

Problem - Certificate Errors!!!

3. Click **View certificate** and check the Issuer: **decrypt.ds.local**

4. Click **Certification Path** and note the red “X” on the root CA

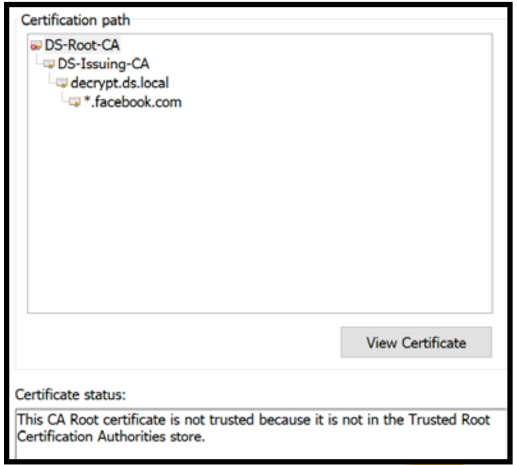


**Certificate Information**

**This certificate cannot be verified up to a trusted certification authority.**

**Issued to:** *.facebook.com

**Issued by:** decrypt.ds.local



Certification path

```
DS-Root-CA
└DS-Issuing-CA
  └decrypt.ds.local
    └*.facebook.com
```

Certificate status:

This CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store.

# Decryption

Ensure CA Is Trusted By All Endpoints

1. There are a number of mechanisms to deploy the certificate to your endpoints:
   1. Push via Active Directory
   2. Push via script from software distribution platform
   3. Push via GlobalProtect agent
   4. Provide root CA download link and instructions on organization website
2. Note: Firefox browser does not use system certificate store/keychain. Your root CA will need to be imported to the Firefox browser manually or via a script—instructions can be found here: [https://wiki.mozilla.org/CA:AddRootToFirefox](https://wiki.mozilla.org/CA:AddRootToFirefox)

# Decryption

Decryption Profiles - Control Your SSL Traffic

- Decryption profiles are attached to decryption policies and can restrict protocol versions and ciphers. Furthermore they can control access to SSL resources based on conditions, such as having an expired certificate

- It is recommended to create two decryption profiles:

  1. An “IT” decryption profile that allows access to untrusted certs for managing appliances with self-signed certificates if needed

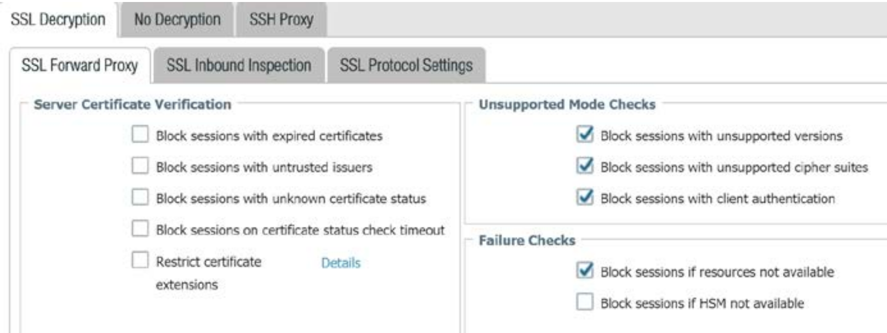
  2. A “Standard” decryption profile that applies to non-IT staff, that will restrict access to untrusted certs

- Each profile should block SSLv3 and TLS v1.0 connections since these are known to be vulnerable and block weak algorithms such as MD5 and RC4

# Decryption

## Decryption Profiles - IT Profile

1. Exceptions made for IT staff that will have to manage appliances that potentially have self-signed certificates



Server Certificate Verification

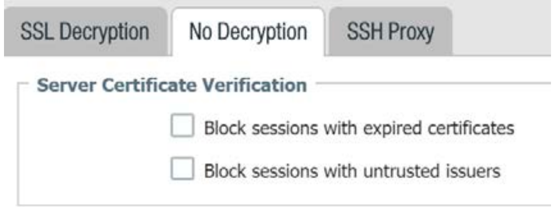
- □ Block sessions with expired certificates
- □ Block sessions with untrusted issuers
- □ Block sessions with unknown certificate status
- □ Block sessions on certificate status check timeout
- □ Restrict certificate extensions Details

Unsupported Mode Checks

- ☑ Block sessions with unsupported versions
- ☑ Block sessions with unsupported cipher suites
- ☑ Block sessions with client authentication

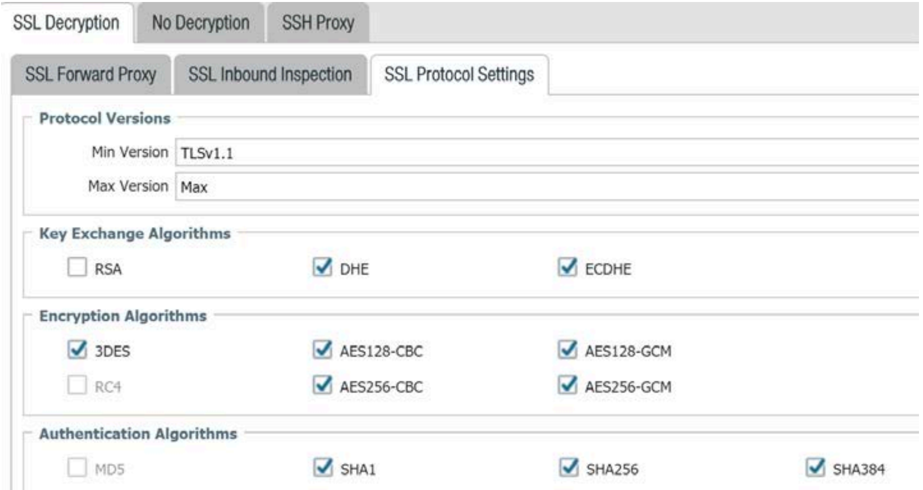
Failure Checks

- ☑ Block sessions if resources not available
- □ Block sessions if HSM not available



Server Certificate Verification

- □ Block sessions with expired certificates
- □ Block sessions with untrusted issuers



Protocol Versions

Min Version TLSv1.1

Max Version Max

Key Exchange Algorithms

□ RSA ☑ DHE ☑ ECDHE

Encryption Algorithms

☑ 3DES ☑ AES128-CBC ☑ AES128-GCM

□ RC4 ☑ AES256-CBC ☑ AES256-GCM

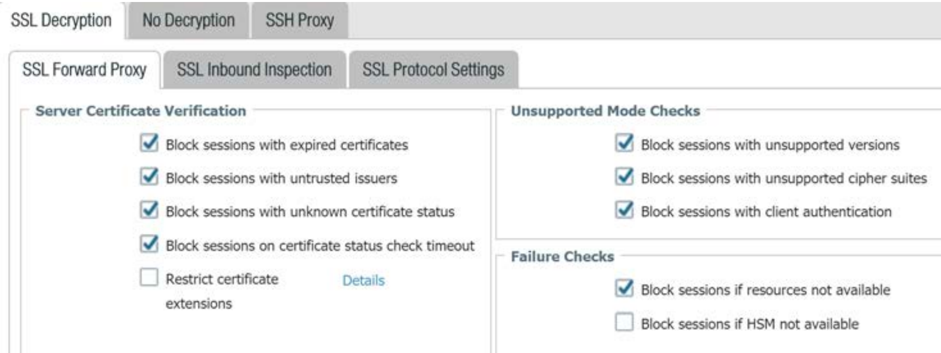
Authentication Algorithms

□ MD5 ☑ SHA1 ☑ SHA256 ☑ SHA384

# Decryption

## Decryption Profiles - Standard Profile

1. No exceptions made—expired, untrusted, and certificates where status cannot be verified (inaccessible CRL/OCSP) will be blocked



**Server Certificate Verification**

☑ Block sessions with expired certificates

☑ Block sessions with untrusted issuers

☑ Block sessions with unknown certificate status

☑ Block sessions on certificate status check timeout

□ Restrict certificate extensions   Details

**Unsupported Mode Checks**

☑ Block sessions with unsupported versions

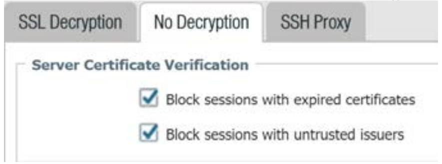
☑ Block sessions with unsupported cipher suites

☑ Block sessions with client authentication

**Failure Checks**

☑ Block sessions if resources not available

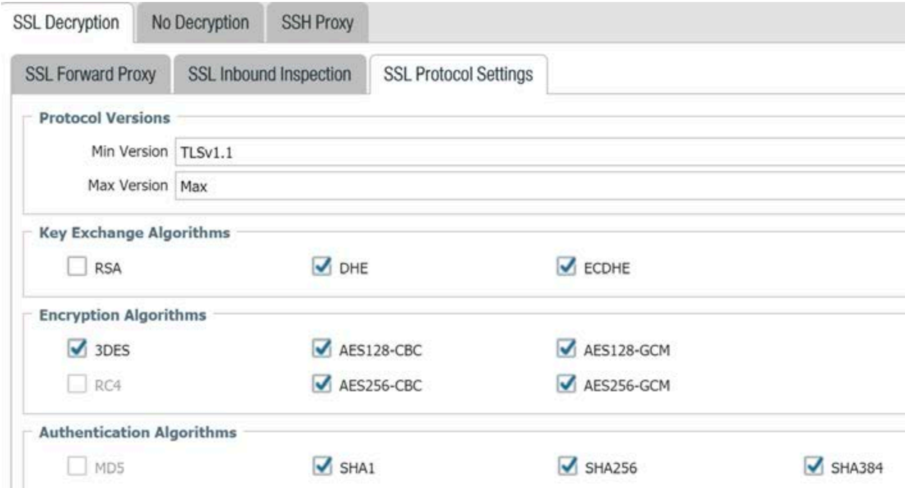
□ Block sessions if HSM not available



**Server Certificate Verification**

☑ Block sessions with expired certificates

☑ Block sessions with untrusted issuers



**Protocol Versions**

Min Version: TLSv1.1

Max Version: Max

**Key Exchange Algorithms**

□ RSA ☑ DHE ☑ ECDHE

**Encryption Algorithms**

☑ 3DES ☑ AES128-CBC ☑ AES128-GCM

□ RC4 ☑ AES256-CBC ☑ AES256-GCM

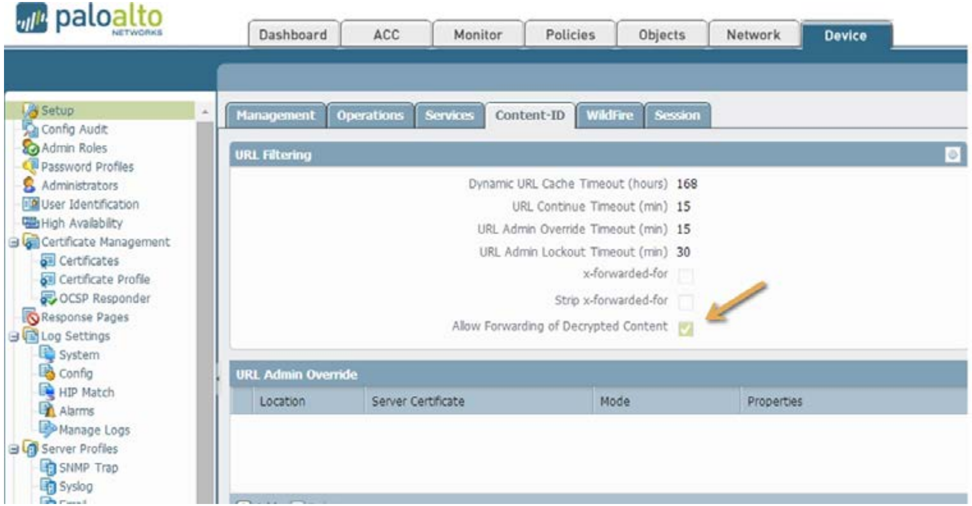
**Authentication Algorithms**

□ MD5 ☑ SHA1 ☑ SHA256 ☑ SHA384

# Decryption

Forward Decrypted Files to Wildfire

1. When decrypt is used, make sure to check “Allow Forwarding of Decrypted Content”
2. Device > Setup > Content-ID > URL Filtering
3. Note: this cannot be pushed via Panorama—must be configured on the firewall



URL Filtering

Dynamic URL Cache Timeout (hours) 168
URL Continue Timeout (min) 15
URL Admin Override Timeout (min) 15
URL Admin Lockout Timeout (min) 30
x-forwarded-for □
Strip x-forwarded-for □
Allow Forwarding of Decrypted Content ☑

URL Admin Override

| Location | Server Certificate | Mode | Properties |
|---|---|---|---|

# Decryption

## Troubleshooting Methods

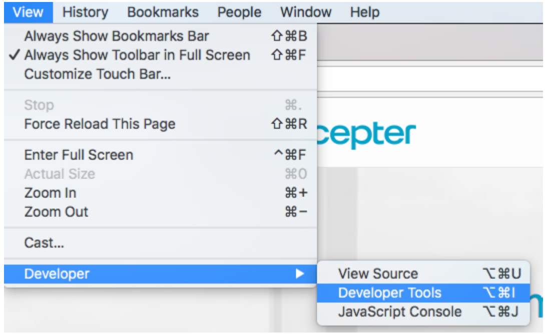
- For any decryption problem, first verify the right certificate is being used or is installed
- Exclusion list in 8.0
- Use external dynamic lists to automate exclusions
- Traffic logs now show decrypt failure causes

## County's Prospective

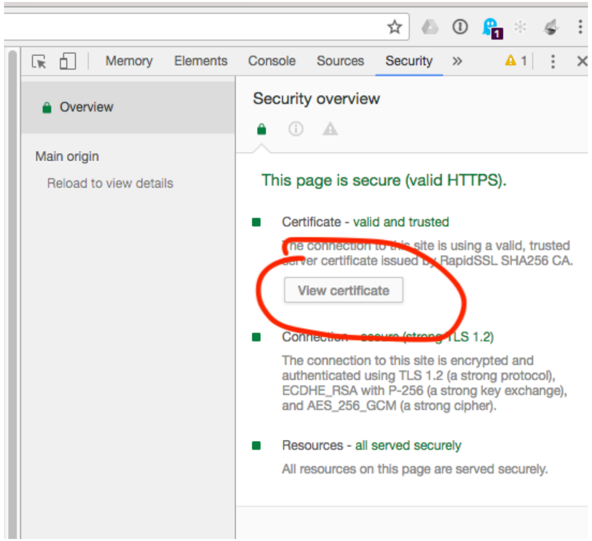
- Corrupted GPO file prevented SSL certificate to be used
- AD structure – users in the right OU's
- Dept with OU's that include all users
- Have network/security staff available to troubleshoot after SSL is turned on
- Inform Service Desk of schedule
- Remove user from SSL
- Limit the pain – if xx number of user are having issues turn off SSL

# Decryption

## How to View Certificate in Chrome



1. Open developer tools.



Security overview

This page is secure (valid HTTPS).

Certificate - valid and trusted

The connection to this site is using a valid, trusted server certificate issued by RapidSSL SHA256 CA.

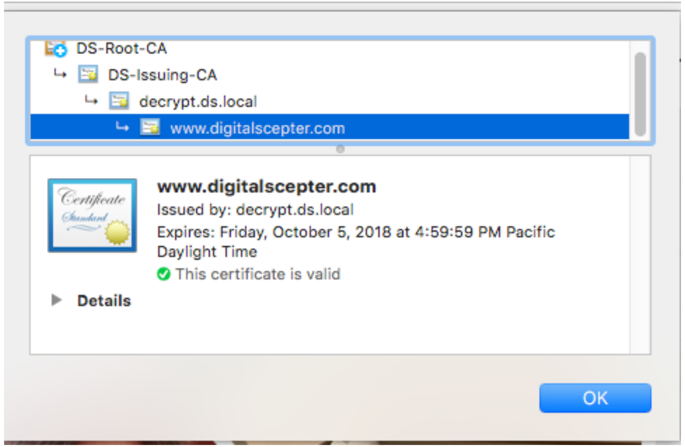
Connection - secure (strong TLS 1.2)

The connection to this site is encrypted and authenticated using TLS 1.2 (a strong protocol), ECDHE_RSA with P-256 (a strong key exchange), and AES_256_GCM (a strong cipher).

Resources - all served securely

All resources on this page are served securely.

2. View certificate



**www.digitalscepter.com**

Issued by: decrypt.ds.local

Expires: Friday, October 5, 2018 at 4:59:59 PM Pacific Daylight Time

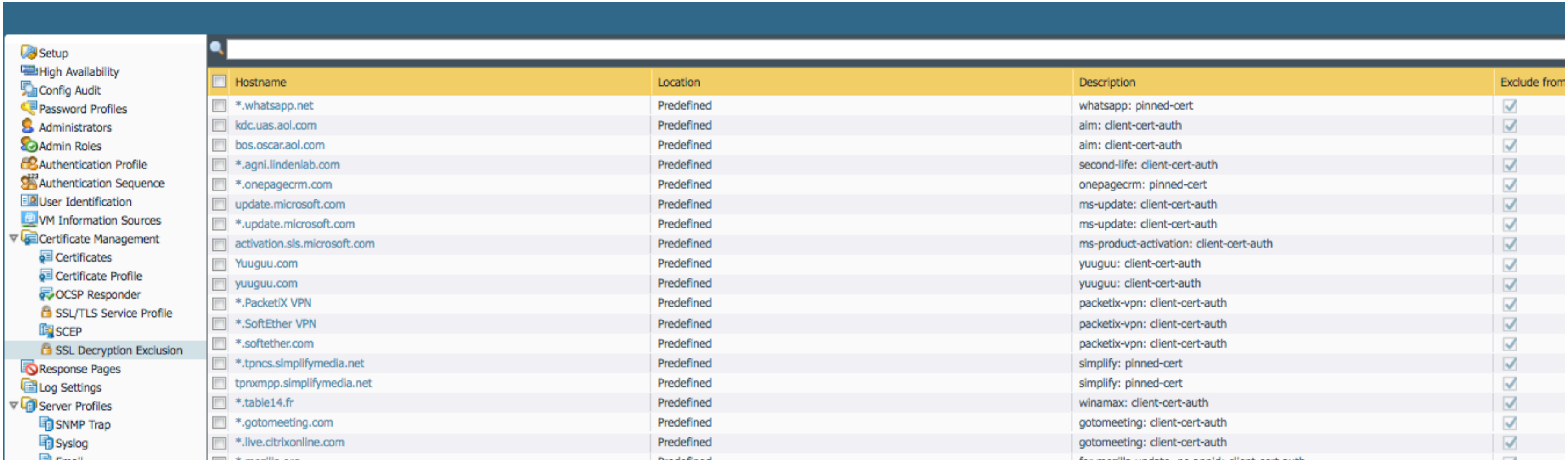
✓ This certificate is valid

3. Verify it’s the firewall CA that issued the cert

# Decryption

## Exclusion List in 8.0

Built in list of sites that can’t be decrypted.  You can now add to this list via the GUI.



| □ | Hostname | Location | Description | Exclude from |
|---|---|---|---|---|
| □ | *.whatsapp.net | Predefined | whatsapp: pinned-cert | ☑ |
| □ | kdc.uas.aol.com | Predefined | aim: client-cert-auth | ☑ |
| □ | bos.oscar.aol.com | Predefined | aim: client-cert-auth | ☑ |
| □ | *.agni.lindenlab.com | Predefined | second-life: client-cert-auth | ☑ |
| □ | *.onepagecrm.com | Predefined | onepagecrm: pinned-cert | ☑ |
| □ | update.microsoft.com | Predefined | ms-update: client-cert-auth | ☑ |
| □ | *.update.microsoft.com | Predefined | ms-update: client-cert-auth | ☑ |
| □ | activation.sls.microsoft.com | Predefined | ms-product-activation: client-cert-auth | ☑ |
| □ | Yuuguu.com | Predefined | yuuguu: client-cert-auth | ☑ |
| □ | yuuguu.com | Predefined | yuuguu: client-cert-auth | ☑ |
| □ | *.PacketiX VPN | Predefined | packetix-vpn: client-cert-auth | ☑ |
| □ | *.SoftEther VPN | Predefined | packetix-vpn: client-cert-auth | ☑ |
| □ | *.softether.com | Predefined | packetix-vpn: client-cert-auth | ☑ |
| □ | *.tpncs.simplifymedia.net | Predefined | simplify: pinned-cert | ☑ |
| □ | tpnxmpp.simplifymedia.net | Predefined | simplify: pinned-cert | ☑ |
| □ | *.table14.fr | Predefined | winamax: client-cert-auth | ☑ |
| □ | *.gotomeeting.com | Predefined | gotomeeting: client-cert-auth | ☑ |
| □ | *.live.citrixonline.com | Predefined | gotomeeting: client-cert-auth | ☑ |

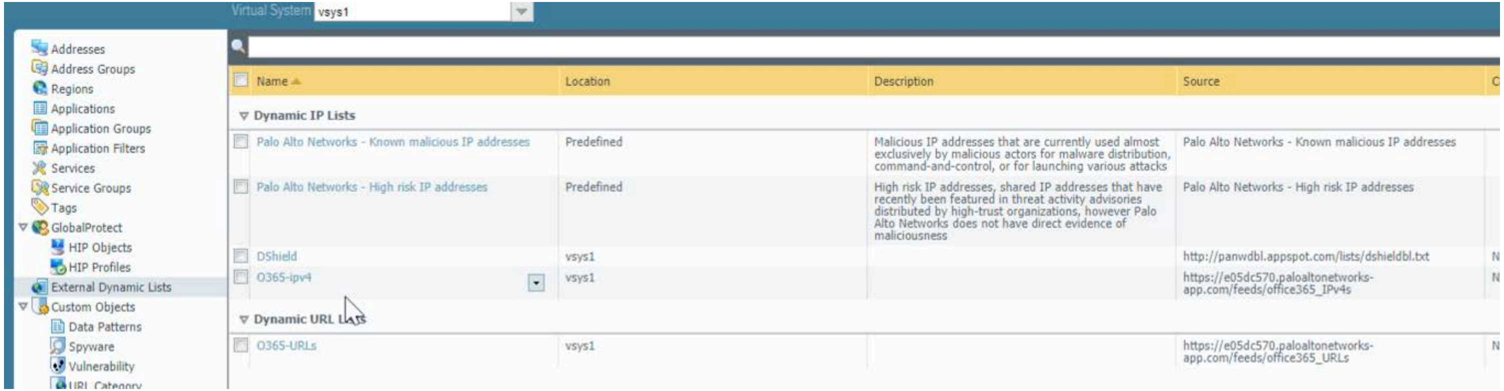
# Decryption

## Use Minemeld to create dynamic list of Microsoft infrastructure IPs

This helps with whitelisting Microsoft properties

Output link of Minemeld to use in external dynamic list to exclude from SSL

Decryption https://e05dc570.paloaltonetworks-app.com/feeds/office365_IPv4s



Virtual System vsys1

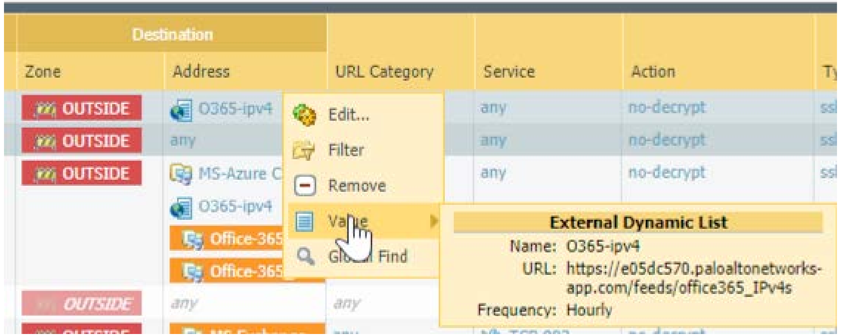
| | Name | Location | Description | Source | C |
|---|---|---|---|---|---|
| | **Dynamic IP Lists** | | | | |
| □ | Palo Alto Networks - Known malicious IP addresses | Predefined | Malicious IP addresses that are currently used almost exclusively by malicious actors for malware distribution, command-and-control, or for launching various attacks | Palo Alto Networks - Known malicious IP addresses | |
| □ | Palo Alto Networks - High risk IP addresses | Predefined | High risk IP addresses, shared IP addresses that have recently been featured in threat activity advisories distributed by high-trust organizations, however Palo Alto Networks does not have direct evidence of maliciousness | Palo Alto Networks - High risk IP addresses | |
| □ | DShield | vsys1 | | http://panwdbl.appspot.com/lists/dshieldbl.txt | N |
| □ | O365-ipv4 | vsys1 | | https://e05dc570.paloaltonetworks-app.com/feeds/office365_IPv4s | N |
| | **Dynamic URL Lists** | | | | |
| □ | O365-URLs | vsys1 | | https://e05dc570.paloaltonetworks-app.com/feeds/office365_URLs | N |

# Decryption

## Use Minemeld to create dynamic list of Microsoft infrastructure IPs

This helps with whitelisting Microsoft properties

Reference the EDL in the destination of a no-decrypt rule and it maintains itself through Minemeld.



| Destination | | | | | |
|---|---|---|---|---|---|
| Zone | Address | URL Category | Service | Action | Ty |
| OUTSIDE | O365-ipv4 | | any | no-decrypt | ssl |
| OUTSIDE | any | | any | no-decrypt | ssl |
| OUTSIDE | MS-Azure C<br>O365-ipv4<br>Office-365<br>Office-365 | | any | no-decrypt | ssl |
| OUTSIDE | any | any | | | |

**External Dynamic List**

Name: O365-ipv4
URL: https://e05dc570.paloaltonetworks-app.com/feeds/office365_IPv4s
Frequency: Hourly

# Decryption

## Decryption End Reasons in Logs

| End reason | Decrypt profile control | Decrypt mode | Troubleshooting action |
|---|---|---|---|
| decrypt-cert-validation | - Expired certificate<br>- Untrusted issuer<br>- Unknown certificate status<br>- Certificate status timeout<br>- Client authentication | - Forward proxy | - Analyze server sent cert chain<br>- Check firewall trust list<br>- Verify OCSP responder connectivity<br>- Look for client certificates |
| decrypt-unsupport-param | - Unsupported protocol<br>- Unsupported cipher<br>- Unsupported SSH algorithm | - Forward proxy<br>- Inbound<br>- SSH proxy | - Run cipher scan on server<br>- Cross check configured ciphers and version |
| decrypt-error | - Resources unavailable<br>- HSM unavailable<br>- SSH errors | - Forward proxy<br>- Inbound<br>- SSH proxy | - Check SSL buffers and sessions on firewall |

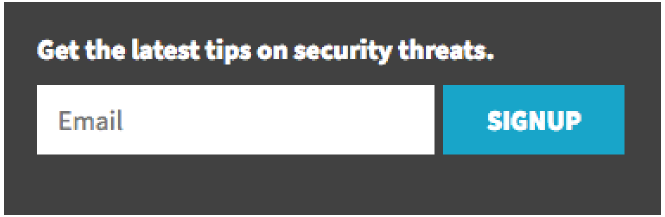
# Decryption

Thank you for attending.

Questions?

Call 1 (888) 299-3718
Email support@digitalscepter.com

Sign up for our newsletter at
https://digitalscepter.com



Get the latest tips on security threats.