



# Citrix XenMobile Enterprise Edition

Claudio Mascaro  
Senior Systems Engineer  
BCD-Sintrag AG

Daniel Kuenzli  
Senior Systems Engineer  
Citrix Systems GmbH

# EMM

Enterprise Mobility Management



Productivity and  
Collaboration



Data Management

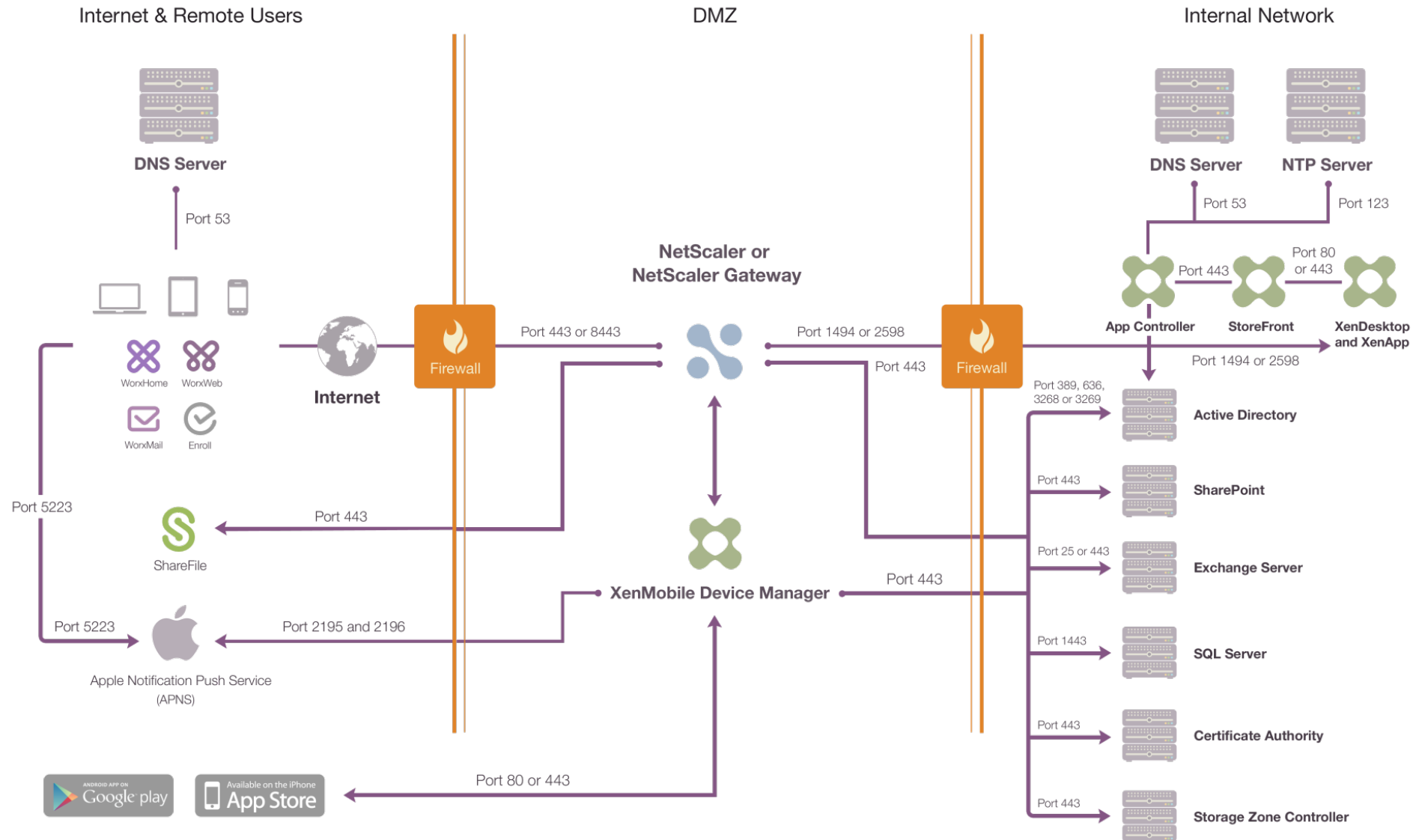


App Management



Device Management

# Technical Preparation: Architecture



# What's new in XenMobile 9.0

# New in XenMobile 9.0 - Platform

XDM cluster simplification

Expanded MDM support for Win 8.1 (Phone and Tablet)

Sony MDM extensions

Modified license files with Citrix v6 compatibility

Support options and TaaS Integration

NetScaler 10.5 – Simpler configuration for XenMobile

# What's new in XenMobile 9.0

## Redesigned Worx Apps



### WorxMail

- Simpler navigation
- Fast triage
- iOS background mode
- Admin notification control
- Server-side search (iOS)
- Landscape/Portrait



### WorxWeb

- Consistent look/feel
- Offline page support
- Download persistence



### ShareFile

- Secure EFSS
- Mobile content editing
- SharePoint & network files



### WorxNotes

- Secure notes
- Team notebooks
- Email and calendar integration



### WorxEdit

- Offline content edit
- Review, comment and collaborate on documents



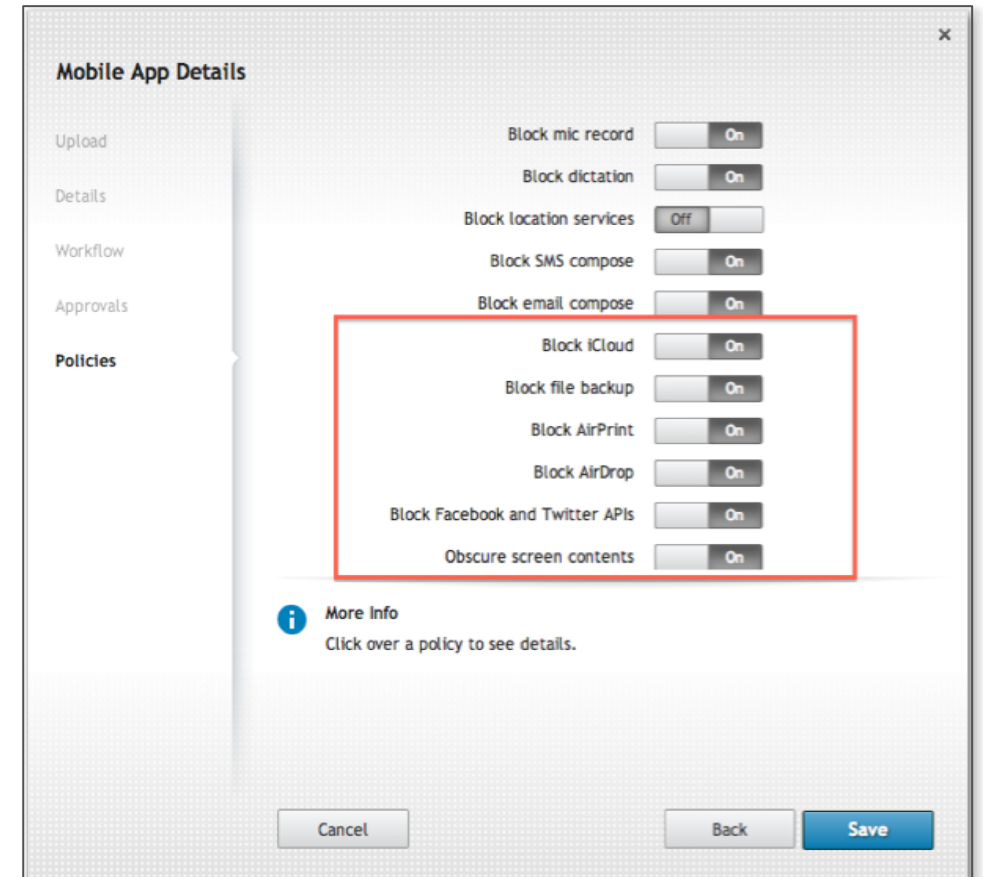
### WorxDesktop

- Secure VDI like access to physical desktop
- Access work files and apps

# 9.0 MDX security enhancements

## New containerization policies

- Prevent backup to iCloud
- Prevent file backup
- Block Airprint
- Block AirDrop/NFC
- Block Social Features
- App screen is obscured when it goes to background



# Infrastructure and Client Considerations



# Key XenMobile Concepts

Enrollment considerations

WorxWeb SSO and Proxy considerations

WorxMail, STA, microVPN and Battery

Certificates and PKI

iOS 8 support considerations

Secrets Vault and User Entropy

SSL Settings on NetScaler and Troubleshooting

# Enrollment

MDM, MAM, ADS, 2FA, SHP etc

# Enrollment modes and mechanisms

Auto-discovery is easiest for user onboarding

- ADS security setting for public certificate trust (MITM protection)
- MAM only mode supported as well

UPN is recommended for user authentication

- Local users are available for MDM only, but not for MAM and Enterprise
- Explicit UPN gets away from implicit UPN complications

2-factor is available for both MDM and MAM authentication

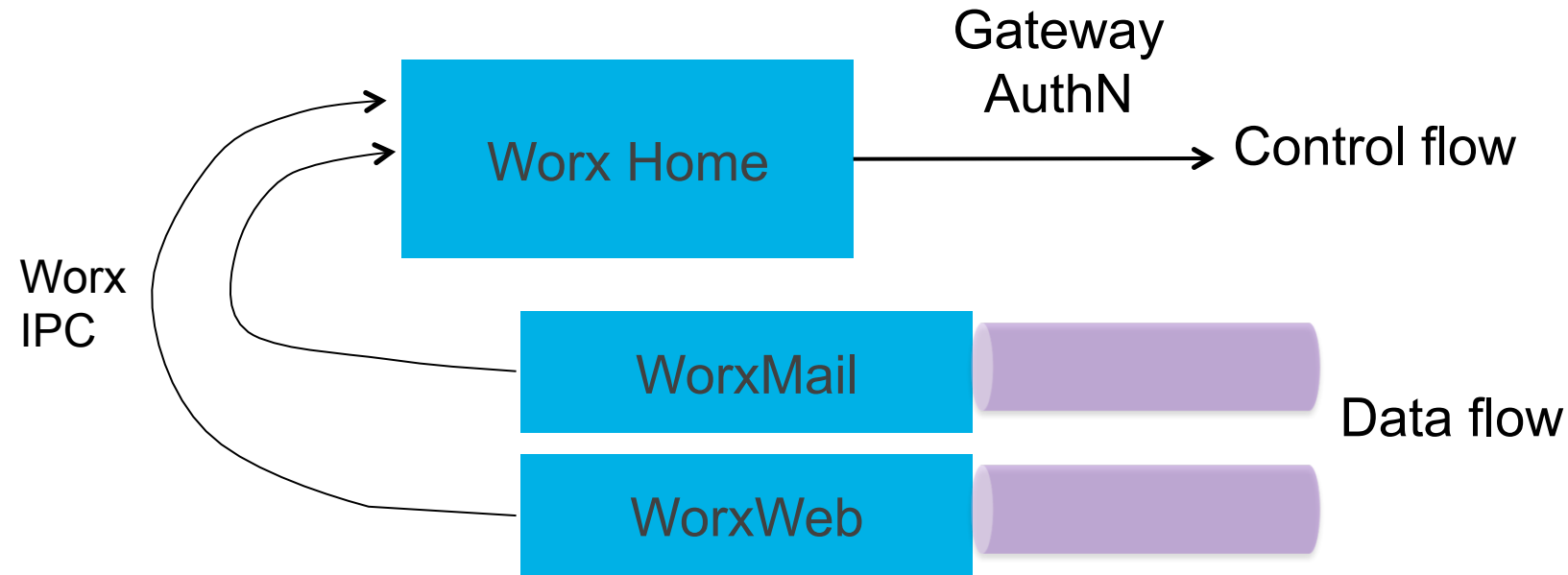
- XenMobile generated OTP for MDM enrollment
- RADIUS OTP support for MAM authentication

Invitation URLs seems popular with customers

- Sent via SMS to user's mobile number from AD
- Self-Help portal for user self-service enrollment

# WorxWeb, Proxy and Topology

## TYPICAL CLIENT INTERACTION - RECAP



- Worx Home responsible for control flow and session ticket generation
  - Responsible for full Gateway authentication at the NetScaler
- Worx apps responsible for data flow with backend servers
  - Only need valid session ticket to open connection to NetScaler (STA or NS\_AAAC)

# WorxWeb Einsatzszenarien

## Infrastruktur

### WorxWeb direkt zu WebServer

- „no-brainer“
- Kein Vorteil für externe Benutzer

### WorxWeb mit mVPN Tunnel

- WorxHome authentifiziert Tunnel
- Benutzer am SSLVPN angemeldet
- HTTPs vom Client zum WebServer
- SSO nur für HTTP möglich

### WorxWeb mit SecureBrowse

- Umschreiben am Client (Aufwand)
- SSO auch für HTTPs möglich



**Network Access**

Network access

**Network Access**

Network access

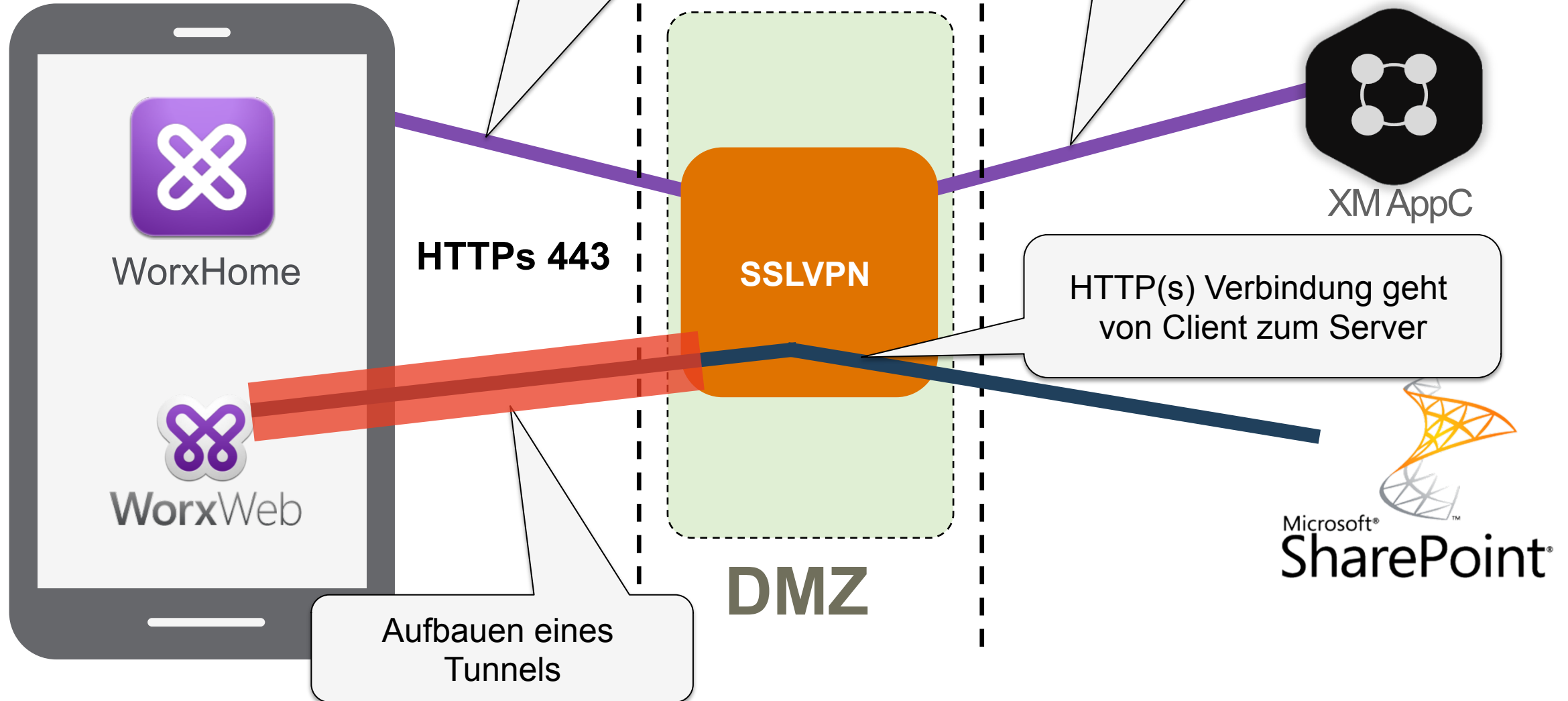
Preferred VPN mode

**Network Access**

Network access

Preferred VPN mode

# WorxWeb



# WorxWeb SSO

Bei HTTPS kein SSO möglich

Bei HTTP beantwortet CNS SSO Request



HTTPS 443

SSLVPN

HTTP401

Bei HTTPS kann Verbindung nicht unterbrochen werden am CNS





# WorxWeb mit SecureBrowse

SecureBrowse schreibt HTTP Traffic **am Client** um

- aus URL: <http://sharepoint/huhu.html> wird  
<https://sslvpn.comp.com/SecureBrowse/http/sharepoint/huhu.html>

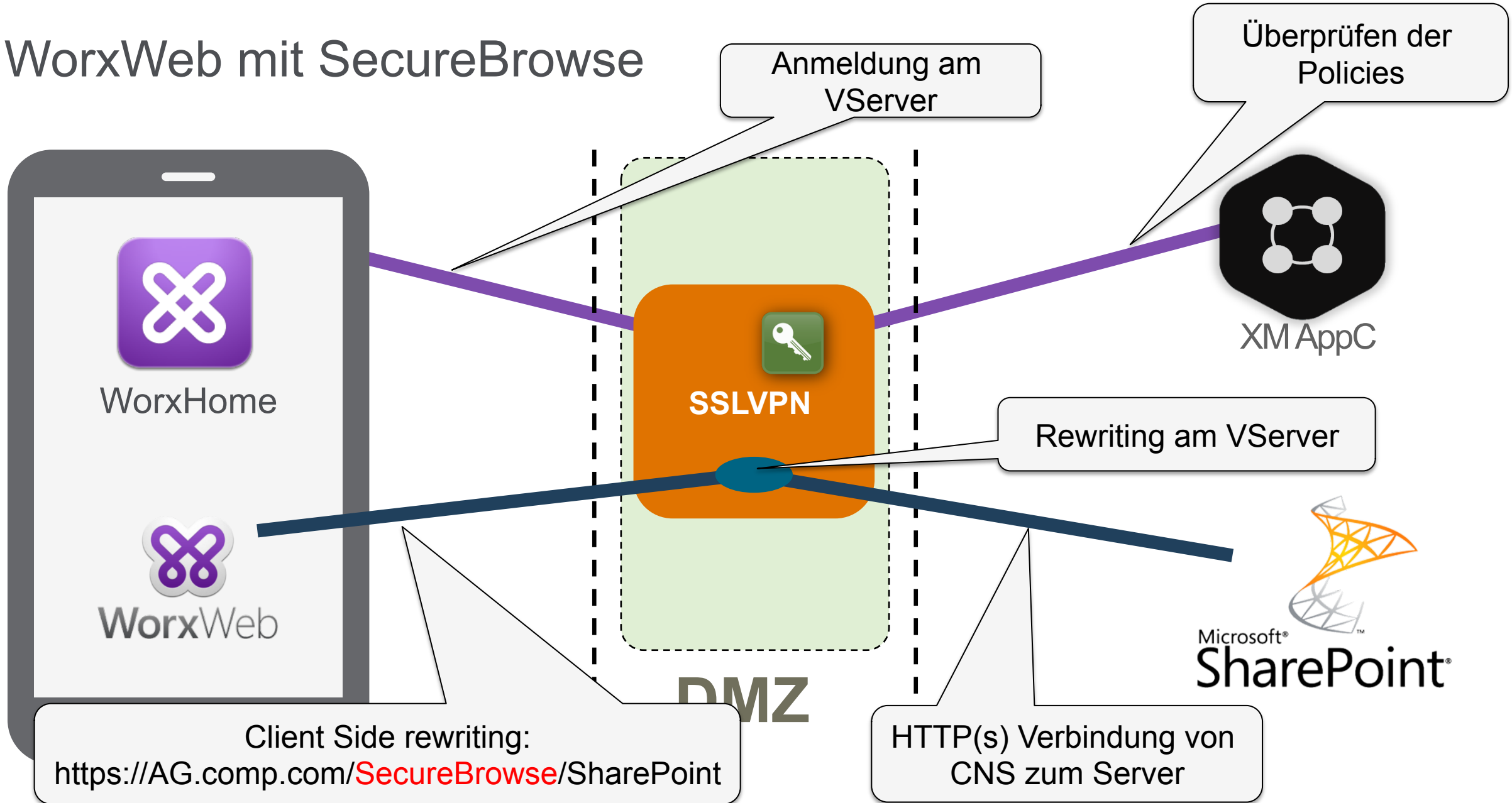
NetScaler ist aus Sicht des WebServers der Client (SSL Verbindung)

NetScaler kann für HTTP und HTTPs SSO Requests beantworten

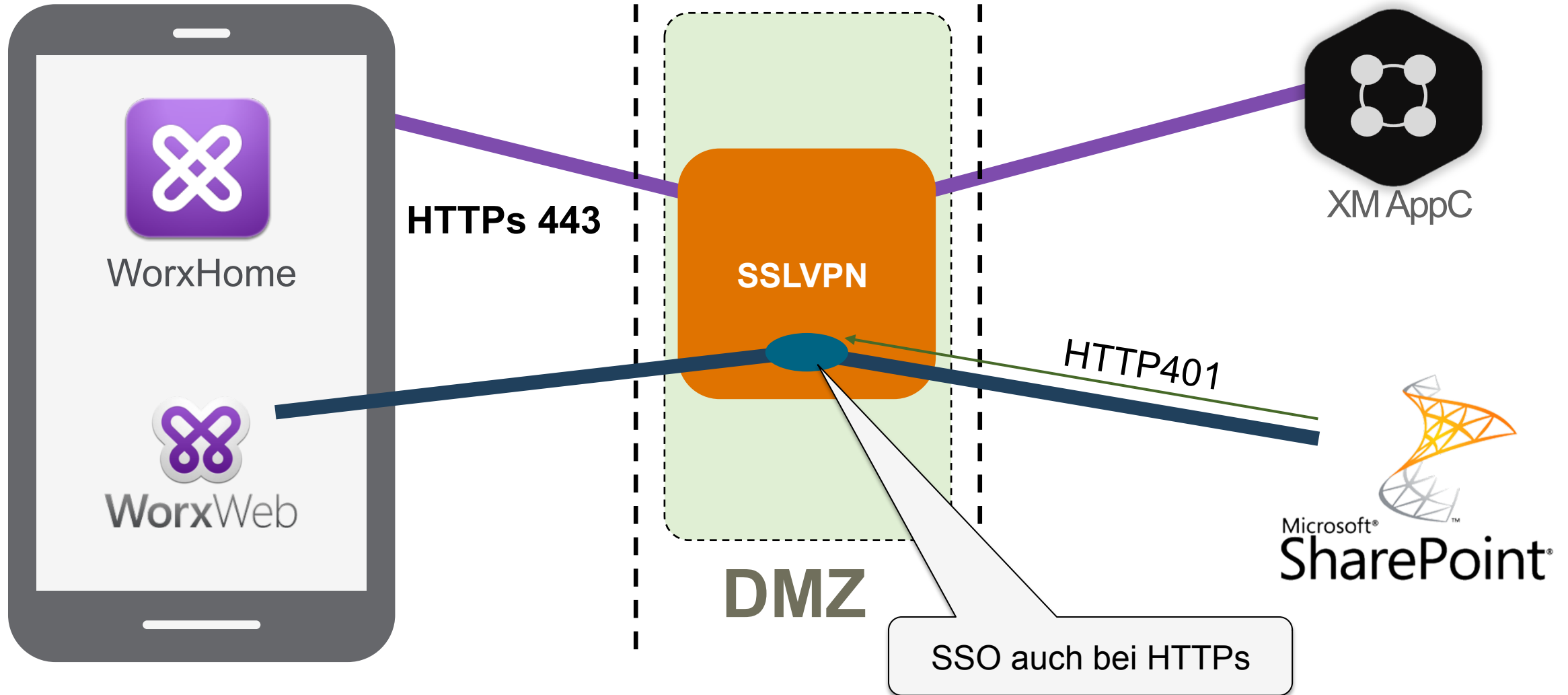
Mehr Rechenaufwand am Browser und am NetScaler als mVPN

Es wird kein Tunnel *offen* gehalten

# WorxWeb mit SecureBrowse

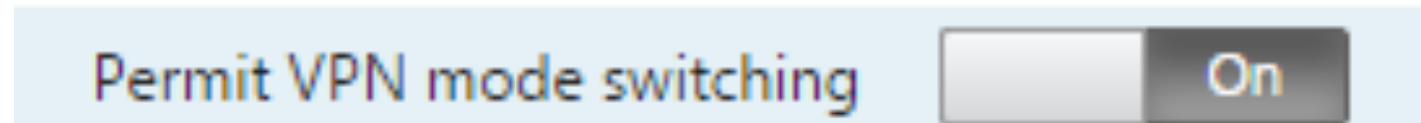


# WorxWeb mit SecureBrowse



# WorxWeb: MicroVPN Flexibility

Permit VPN mode switching

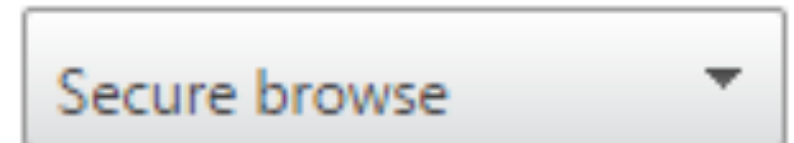
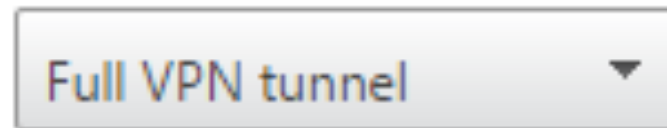


Default: mVPN



Fallback für HTTPs SSO: SecureBrowse

Preferred VPN mode



# Beispiele für HTTP Proxy Traffic Policies (non global)

## Internes WiFi Netz

- **Inter**net Daten gehen über Proxy Server
- **Intra**net Daten gehen direkt zu den Servern

## Proxy für bestimmte Server

Verbindungen zu bestimmten Netz brauche spezielle Settings (proxy/noproxy)

# Proxy global Setzen und Überschreiben für Ausnahmen

```
set vpn parameter -clientIdleTimeout 1 -proxy NS -httpProxy  
10.54.255.155:3128 -sslProxy 10.54.255.155:3128
```

```
add vpn trafficAction allow_intranet_ta http -proxy NOPROXY  
add vpn trafficPolicy Allow_intranet_tp "REQ.IP.DESTIP == 10.0.0.0 -  
netmask 255.0.0.0 || REQ.IP.DESTIP == 162.139.0.0 -netmask 255.255.0.0 ||  
REQ.IP.DESTIP == 142.56.0.0 -netmask 255.255.0.0" allow_intranet_ta
```

## Alternativ:

```
add vpn trafficPolicy bypass_intranet "REQ.HTTP.HEADER CSHOST CONTAINS  
mycompany.com" allow_intranet
```

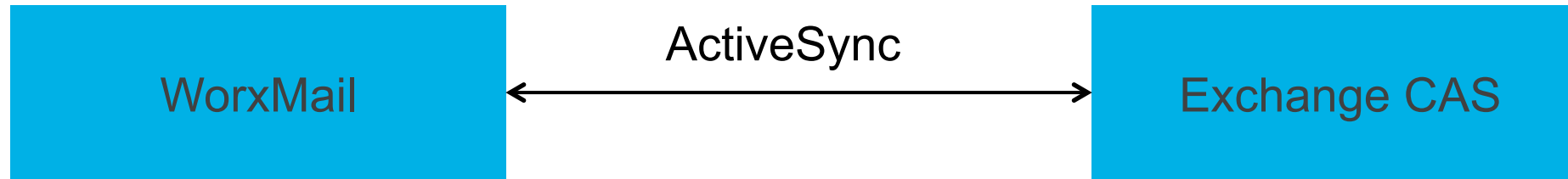
```
bind vpn vserver MyVPN-policy Allow_intranet
```

# WorxWeb with NetScaler Proxy config

|                                    | <u>iOS</u><br><u>SecureBrowse</u> | <u>iOS</u><br><u>MicroVPN</u> | <u>Android</u><br><u>SecureBrowse</u> | <u>Android</u><br><u>MicroVPN</u> |
|------------------------------------|-----------------------------------|-------------------------------|---------------------------------------|-----------------------------------|
| HTTP                               | ✓                                 | ✓                             | ✓                                     | ✓                                 |
| HTTPS                              | ✓                                 | ✓                             | ✓                                     | ✓                                 |
| HTTP w/ 401 SSO                    | ✓                                 | ✓                             | ✓                                     | ✓                                 |
| HTTPS w/401 SSO                    | ✓                                 | x                             | ✓                                     | x                                 |
| HTTP via Proxy                     | ✓                                 | ✓                             | ✓                                     | ✓                                 |
| HTTPS via Proxy                    | x                                 | ✓                             | x                                     | ✓                                 |
| HTTP via proxy w/ 407 SSO          | ✓                                 | ✓                             | ✓                                     | ✓                                 |
| HTTPS via proxy w/ 407 SSO         | x                                 | x                             | x                                     | x                                 |
| HTTP via proxy w/ 407 and 401 SSO  | ✓(NS 10.5)                        | ✓                             | ✓(NS 10.5)                            | ✓                                 |
| HTTPS via proxy w/ 407 and 401 SSO | x                                 | x                             | x                                     | x                                 |

\*Traffic Policies cannot be applied by DestIP in SecureBrowse mode. This is being addressed in the near future.

## SIMPLEST WORXMAIL DEPLOYMENT



MDX Network access = Unrestricted

### Pros

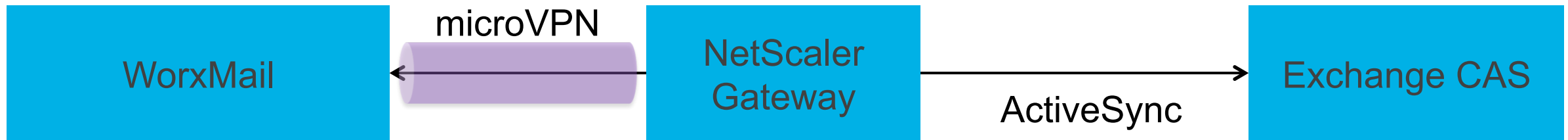
1. Best battery life of device
2. At-rest data security and SSL for transport
3. Client-cert authN for additional security

### Cons

1. ActiveSync Service is internet faced and need to be secured
2. More complex regarding device control



## NON-IDEAL WORXMAIL DEPLOYMENT



MDX Network access = Tunneled

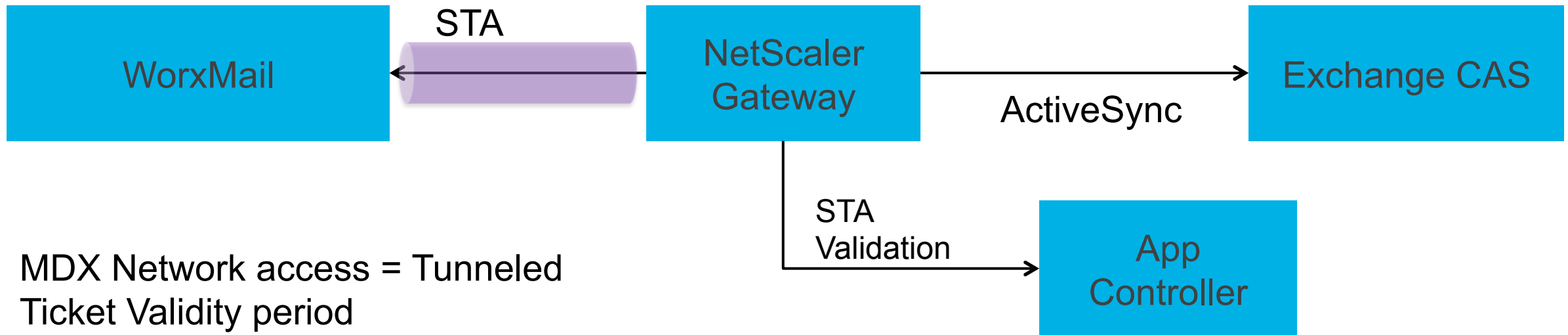
### Pros

1. ActiveSync only in LAN
2. Full control of device access

### Cons

1. Poor device battery life

## RECOMMENDED WORXMAIL DEPLOYMENT

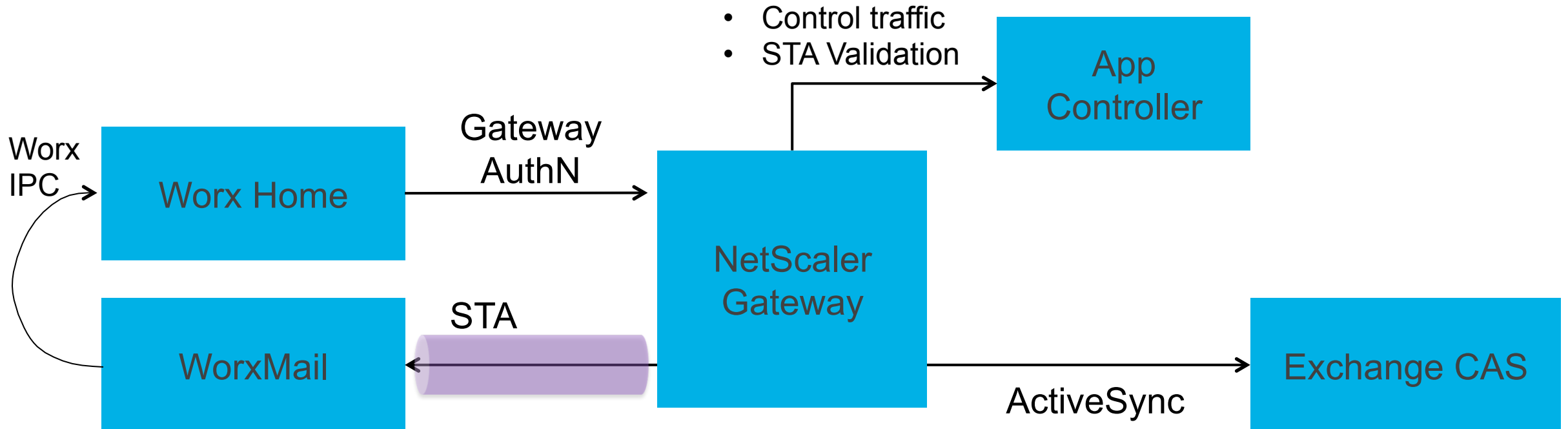


MDX Network access = Tunneled  
Ticket Validity period  
Background services gateway  
STA provider config on NetScaler Gateway

### Pros

1. Best battery performance for most secure deployment
2. Support for client-certs as well
3. Full control of device access

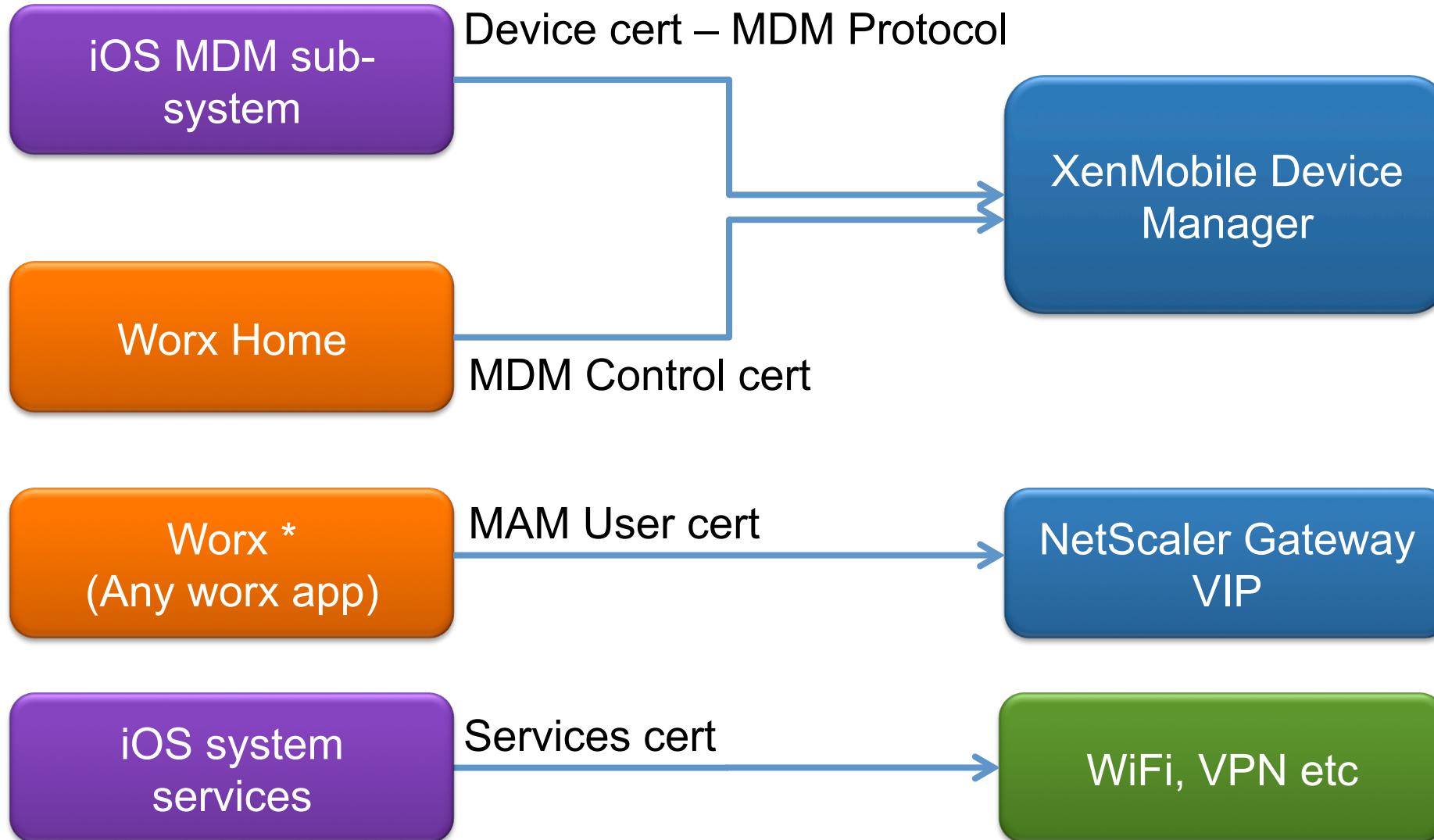
## TRAFFIC FLOW



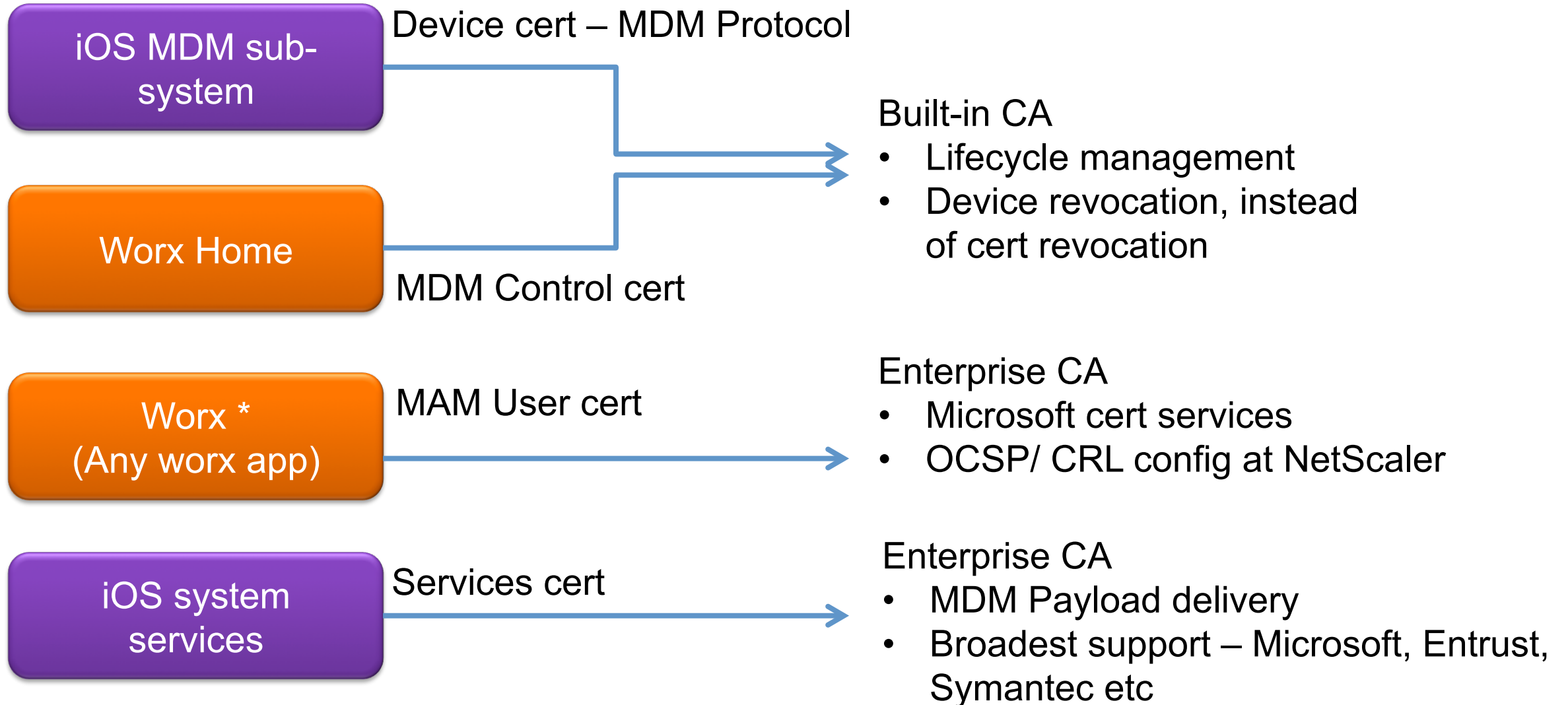
1. Worx Home authN at NetScaler Gateway VIP based on configured authN policy
2. All control communication with App Controller
3. WorxMail token retrieval from Worx Home
4. WorxMail data connection to NetScaler Gateway and onward to CAS

# Certificates and PKI

# Multiple certificates doing multiple things ...



# Multiple certificates doing multiple things ...CAs are different



# iOS 8 compatibility considerations

# Background

MDX leverages dylib for app. policies during wrapping process

iOS 8 now supports App. Extensions with Dylib

Using dylib mandates use of **Team ID** within provisioning profile (malware protection)

Enterprise Certs has an additional field '**Organization unit**' that is required by MDX

- Present from late 2013 onwards



# Solution

Apps need to be re-wrapped using MDX 9.0.2+

Verify signing cert and provisioning profile for team ID and OU

# Check for new Provisioning Profile

```
New_Enterprise_Profile.mobileprovision
list version="1.0">
ict>

<key>AppIDName</key>
<string>Xcode iOS Wildcard App ID</string>

<key>ApplicationIdentifierPrefix</key>
<array>
  <string>9968NABGAS</string>
</array>

<key>CreationDate</key>
<date>2014-08-21T15:52:44Z</date>

<key>DeveloperCertificates</key>
<array>
  ata>MIIFlTCCBH2gAwIBAgIIKdSidnQKrAswDQYJKoZIhvcNAQEFBQAwZyZCZAJBgNVBAYTAlVTMRMwEQYDVQKDApBcHBsZSBSBjBmMuMSwwKgYDVQQLDcNBcHBsZSBSBjBjSjZhdPZGUGRGV2ZWxvcGVyIFJlbGF0aW9uczcFEMEIGA1U
  ww7QXBwbGUGV29ybGR3aWRlIERldmVs3B3BlciBSZwXhdGlvbnMgQ2VydGlmawNhdGlvbiBBdXRob3JpdHkwHhcNMTQwODIxMTU0MDUyWjCBiDEaMBGCGmSjJomT8ixkAQEMCjk5Njh0QUJHQVMxNDAYBgNV
  MMK2lQaG9uZSBEaXN0cmliXDRpb246IERhdmlkIEhveSAo0Tk20E5BQkdBUyKxEzARBgNVBAsMCjk5Njh0QUJHQVMxZjAQBGNVBAoMCURhdmlkIEhveTElMAkGA1UEBHMCMVVMwggEiMA0GCSqGSIb3DQEBAAQAA4IBDwAwggEKAoIBA
  U3Bkv3MK7bf9WCzQFwEwFVmq7aXBvBCap5wLhCoqRuuTwk0K7CZk0l7U90g9CTb6tSSTz rM/GRzSB5EJv2SREg6VZw1gGkfmgzPDGmpmxEUMp7sxTf9cbp1BfmN6BUYnpN4tu
  Meoa95buJKEM0kZvtQ0DTjMdX2IgUPKpo4I1rxLxqD4wVTlPwHBDvCq94qVYHCcnPNYZEADrvRyBtSlwuU6CqCFgYPCY/
  feIIwdbaFhw6ZmHd9xRlpa0NCZZ40HffKeh0P6uz1ebyMAANo1jKRwKNQG0Z5zq0cyvermN0FFIt734UlzJxhhxcTvRdHJS1ly4e4rLoKmeXrPhAgMBAAGjggHxMIIB7TAdBgNVHQ4EFgQUQCXybmq2EbTJpD4VXZ1czTnecCS4wDAYD
  0TAQH/BAIwADAfBgNVHSMEGDAWgBSIJxcJqbYYYIvs67r2R1nFULSjtZCCAQ8GA1UdIASCAQYwggECMIH/
  kqhkiG92NkBQEWgfEwgMGCCsGAQUFBWICIMIG2DIGzUmVsawFuY2Ug24gdGhpcyBjZXJ0awZpY2F0ZSBSieSBhbnkgcGFydHkgYXNzdW1lcyBhY2NlCHRhbmlIG9mIHRoZSB0aGVuIGFwcGxpY2FibGUgc3RhbmlhcmQgdGVybXMGY
  kIGNvbmlRpdGlvbnMgb2YgdXNlLCBjZXJ0awZpY2F0ZSBSb2x2Y3kgYW5kIGNlcnRpZmljYXRpb24gcHJhY3RpY2Ugc3RhdGVtZW50cy4wKQYIKwYBBQUHAgEWHWh0dHA6Ly93d3cuYXBwbGUuY29tL2FwcGxly2EvME0GA1UdHwRGMG
  QqBAoD6GPgh0dHA6Ly9kZXZlbG9wZXIuYXBwbGUuY29tL2NlcnRpZmljYXRpb25hdXRob3JpdHkwHhcNMTQwODIxMTU0MDUyWjCBiDEaMBGCGmSjJomT8ixkAQEMCjk5Njh0QUJHQVMxNDAYBgNV
  CBQAwDQYJKoZIhvcNAQEFBQADggEBAG8xiUxK+fUjIRlosnc7s81DUCo21Ki7C4ai
  tDtP7Y1dt ryPR0scbQoe08wddauakVMQxUFAnt8t9J0+4iUSqlq4n0muffIqH950nVN3BX8yC0ZbMUw37W5kiU9oII79b6AYXDN5Dw0kx7Xj7a00+AqaSgLESC7t61lzH+bLCdudHNtEgzht8xnL98MiUci1PVVXN3E0/
  LQE9DxNiS8ZrkhY0z/hmN1YC0ghJfso51bycZPJNvBqC+Na0rGmM/26F5zMeZY1PvE+g5/SUyrL8y07T3XuUJdMUy+zFks+62yqPYoreXHMFJ06fm9ICoYAXv5HMx9X3emrZUrzq4g=</data>
</array>

<key>Entitlements</key>
<dict>
  <key>com.apple.developer.ubiquity-kvstore-identifier</key>
  <string>9968NABGAS.*</string>

  <key>com.apple.developer.team-identifier</key>
  <string>9968NABGAS</string>

  <key>keychain-access-groups</key>
  <array>
    <string>9968NABGAS.*</string>
  </array>

  <key>com.apple.developer.ubiquity-container-identifiers</key>
  <array>
    <string>9968NABGAS.*</string>
  </array>
</dict>
</key>
</dict>
</list>
</plist>
```



iPhone Distribution: Citrix Systems, Inc

**iPhone Distribution: Citrix Systems, Inc**  
 Issued by: Apple Worldwide Developer Relations Certification Authority  
 Expires: Saturday, May 7, 2016 at 9:33:00 AM Eastern Daylight Time  
 This certificate is valid

Trust  
 Details

**Old Enterprise Cert.**

Subject Name  
 User ID P2QGLXTE6L  
 Common Name iPhone Distribution: Citrix Systems, Inc  
 Organization Citrix Systems, Inc  
 Country US

Issuer Name  
 Country US  
 Organization Apple Inc.  
 Organizational Unit Apple Worldwide Developer Relations  
 Common Name Apple Worldwide Developer Relations Certification Authority

Serial Number 9148798117156490031  
 Version 3

Signature Algorithm SHA-1 with RSA Encryption ( 1.2.840.113549.1.1.5 )  
 Parameters none

Not Valid Before Wednesday, May 8, 2013 at 9:33:00 AM Eastern Daylight Time  
 Not Valid After Saturday, May 7, 2016 at 9:33:00 AM Eastern Daylight Time

Public Key Info

iPhone Developer: Jessie Qiu (36MMA2ASQC)

**iPhone Developer: Jessie Qiu (36MMA2ASQC)**  
 Issued by: Apple Worldwide Developer Relations Certification Authority  
 Expires: Wednesday, December 3, 2014 at 3:52:50 PM Eastern Standard Time  
 This certificate is valid

Trust  
 Details

**New Enterprise Cert.**

Subject Name  
 User ID R7ETNGBBQA  
 Common Name iPhone Developer: Jessie Qiu (36MMA2ASQC)  
 Organizational Unit KBVSJ83SS9  
 Organization Citrix Systems, Inc.  
 Country US

Issuer Name  
 Country US  
 Organization Apple Inc.  
 Organizational Unit Apple Worldwide Developer Relations  
 Common Name Apple Worldwide Developer Relations Certification Authority

Serial Number 5633530735228874154  
 Version 3

Signature Algorithm SHA-1 with RSA Encryption ( 1.2.840.113549.1.1.5 )  
 Parameters none

Not Valid Before Tuesday, December 3, 2013 at 3:52:50 PM Eastern Standard Time  
 Not Valid After Wednesday, December 3, 2014 at 3:52:50 PM Eastern Standard Time

Public Key Info  
 Algorithm RSA Encryption ( 1.2.840.113549.1.1.1 )  
 Parameters none

## Log file

MySample(pid 964) - [deny-mmap] mapped file has no team identifier and is not a platform binary:

# Secrets Vault

User Entropy, System Entropy etc

# What Secrets?

Certificate

Cached AD  
Password

Exchange  
Server IP

User Name

NetScaler  
Cookie

# Secrets are stored in iOS KeyChain

Worx Home

| Key          | Value |
|--------------|-------|
| Crypto_S1    | ...   |
| Crypto_S2    | ...   |
| NS_AAAC      | ...   |
| P12_Password | ...   |
| SAML_Token   | ...   |

WorxMail

| Key      | Value |
|----------|-------|
| CAS_FQDN | ...   |
| Email    | ...   |
| Password | ...   |

WorxWeb

| Key | Value |
|-----|-------|
| ??? | ...   |
| ??? | ...   |
| ??? | ...   |

# Isn't OS secure-storage safe?

## Yes & No

### Yes

- KeyChain encrypted with Device Pin
- Enforce Device Pin for Corporate owned devices

### No

- Device Pin for BYOC?
- Users don't set strong Device Pins
- Jailbreak or Rooted device – Storage is easily accessible

# So what do we do?

## Secrets Vault

- Encrypted storage built on top of OS secure-store
- Accessible to WorxHome & all MDX apps
- Secures all secrets – sensitive material that may be leveraged for an exploit / privacy

### Worx Home

- K1 = Device random value
- K2 = Vendor specific value
- K3 = Device Identifier

| Key           | Value   |
|---------------|---|
| Key Vault     | Key=Enc(K1, K2, K3)                           |
| Secrets Vault | Enc((S1, S2,Cert_Key,NS_AAC, SAML_Token),Key) |



# That's Secure

Yes – Strong proprietary encryption, on top of OS protection

If device stolen:

- 1<sup>st</sup> hurdle – Jailbreak device and access KeyChain
- 2<sup>nd</sup> hurdle – Identify the right element in keychain for attack
- 3<sup>rd</sup> hurdle – Secrets Vault appears to be a meaningless blob
- 4<sup>th</sup> hurdle – Reverse Engineer WorxHome code to figure out the layered encryptions, and various keys used

Attack – **Theoretically Possible, Practically Very Hard**

Problem – **All elements required for decryption, reside on the device**

# User Entropy

App Controller setting = Enable secrets using passcode

Introduce new variable, that never resides on the device

WorxPin – Pin known only to user (Recommended)

- Used for all offline MDX authentication
- Used for introducing new randomness into Secrets Vault protection

AD Password

- Also possible to use AD password as UE

# Secrets Vault – with User Entropy

- K1 = Device random value
- K2 = Vendor specific value
- K3 = **User Entropy**

| Key           | Value   |
|---------------|---|
| Key Vault     | Key=Enc(K1, K2, K3)                           |
| Secrets Vault | Enc((S1, S2,Cert_Key,NS_AAC, SAML_Token),Key) |

**User Entropy = WorxPin / AD Password**

(only user knows UE – Stolen device can not decrypt data)

# SSL Cheats on NetScaler

# How to get better rating on your SSL Vserver

Result with standard NetScaler Gateway configuration



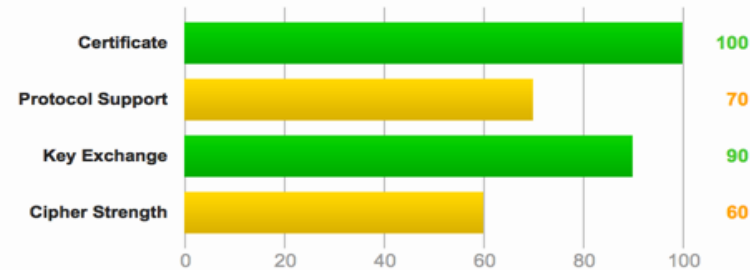
## SSL Report: 46-16-186-50.mycitrixdemo.net (46.16.186.50)

Assessed on: Fri Oct 17 02:31:51 PDT 2014 | [Clear cache](#)

[Scan Another »](#)

### Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).



This server uses SSL 3, with POODLE mitigated. Still, it's recommended that this protocol is disabled. [MORE INFO »](#)

Certificate uses SHA1. When renewing, ensure you upgrade to SHA256. [MORE INFO »](#)

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to B.

The server does not support Forward Secrecy with the reference browsers. [MORE INFO »](#)

# Weak Ciphers and Poodle Attack vulnerability


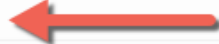
| Configuration   |   |     |
|---|---|-----|
|  | <b>Protocols</b>  |     |
|   | TLS 1.2   | No  |
|   | TLS 1.1   | No  |
|   | TLS 1.0   | Yes |
|   | SSL 3 <b>INSECURE</b>   | Yes |
|   | SSL 2   | No  |
|  | <b>Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites always at the end)</b> |     |
|   | TLS_RSA_WITH_RC4_128_MD5 (0x4)  | 128 |
|   | TLS_RSA_WITH_RC4_128_SHA (0x5)  | 128 |
|   | TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)   | 112 |
|   | TLS_RSA_WITH_DES_CBC_SHA (0x9) <b>WEAK</b>  | 56  |
|   | TLS_RSA_WITH_AES_256_CBC_SHA (0x35)   | 256 |
|   | TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)   | 128 |
|   | TLS_RSA_WITH_DES_CBC_SHA (0x9) <b>WEAK</b>  | 56  |



# No Perfect Forward Secrecy but finally no Renegotiation



## Protocol Details

|   |   |
|---|---|
| <b>Secure Renegotiation</b>             | <b>Supported</b>                              |
| Secure Client-Initiated Renegotiation   | No  |
| Insecure Client-Initiated Renegotiation | No  |
| BEAST attack                            | Mitigated server-side ( <a href="#">more info</a> ) SSL 3: 0x4, TLS 1.0: 0x4  |
| POODLE attack                           | No, mitigated ( <a href="#">more info</a> ) SSL 3: 0x4  |
| <b>Downgrade attack prevention</b>      | <b>No, TLS_FALLBACK_SCSV not supported</b> ( <a href="#">more info</a> )  |
| TLS compression                         | No  |
| RC4                                     | Yes (not with TLS 1.1 and newer) ( <a href="#">more info</a> )  |
| Heartbeat (extension)                   | No  |
| Heartbleed (vulnerability)              | No ( <a href="#">more info</a> )  |
| OpenSSL CCS vuln. (CVE-2014-0224)       | No ( <a href="#">more info</a> )  |
| <b>Forward Secrecy</b>                  | <b>No WEAK</b> ( <a href="#">more info</a> )  |
| Next Protocol Negotiation               | No  |
| Session resumption (caching)            | Yes   |
| Session resumption (tickets)            | No  |
| OCSP stapling                           | No  |
| Strict Transport Security (HSTS)        | No  |
| Long handshake intolerance              | No  |
| TLS extension intolerance               | No  |
| TLS version intolerance                 | TLS 1.3 TLS 1.98 TLS 2.98   |
| SSL 2 handshake compatibility           | Yes   |


### Change Advanced SSL Settings

SSL quantum size (KBytes)  
8

Max CRL memory size (MBytes)  
256

Encryption trigger timeout (10 ms ticks)  
100

Encryption trigger packet count  
45

Deny SSL Renegotiation  
FRONTEND\_CLIENT   
NO  
FRONTEND\_CLIENT  
FRONTEND\_CLIENTSERVER  
ALL  
NONSECURE  
Unicode

PUSH encryption trigger timeout (ms)  
1

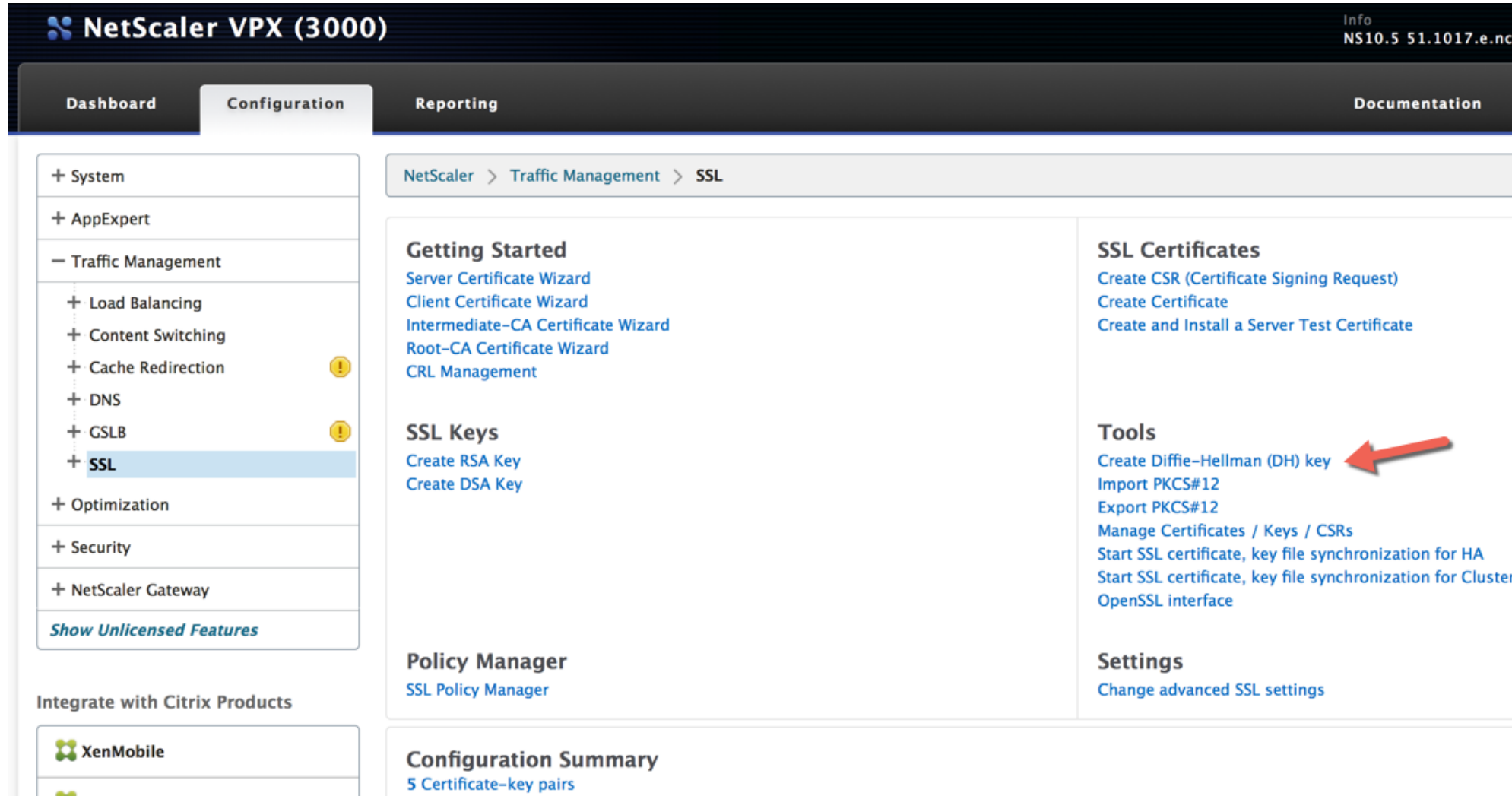
Crypto Device Disable Limit  
0

Undefined Control Action  
CLIENTAUTH

Undefined Data Action  
NOOP

Strict CA checks  Send Close-Notify  
 Drop requests for SNI enabled SSL sessions if host header is absent

# Generating DH Key for FS



The screenshot shows the NetScaler VPX (3000) configuration interface. The breadcrumb navigation is **NetScaler > Traffic Management > SSL**. The left sidebar shows the navigation menu with **SSL** selected under Traffic Management. The main content area is divided into three columns:

- Getting Started**
  - [Server Certificate Wizard](#)
  - [Client Certificate Wizard](#)
  - [Intermediate-CA Certificate Wizard](#)
  - [Root-CA Certificate Wizard](#)
  - [CRL Management](#)
- SSL Keys**
  - [Create RSA Key](#)
  - [Create DSA Key](#)
- Policy Manager**
  - [SSL Policy Manager](#)
- Configuration Summary**
  - [5 Certificate-key pairs](#)
- SSL Certificates**
  - [Create CSR \(Certificate Signing Request\)](#)
  - [Create Certificate](#)
  - [Create and Install a Server Test Certificate](#)
- Tools**
  - [Create Diffie-Hellman \(DH\) key](#) (indicated by a red arrow)
  - [Import PKCS#12](#)
  - [Export PKCS#12](#)
  - [Manage Certificates / Keys / CSRs](#)
  - [Start SSL certificate, key file synchronization for HA](#)
  - [Start SSL certificate, key file synchronization for Cluster](#)
  - [OpenSSL interface](#)
- Settings**
  - [Change advanced SSL settings](#)





# Vserver SSL settings

### Configure SSL DH Param

DH Filename (with path)  
  ▼

DH Parameter Size (Bits)  
 ?

DH Generator  
 2  5

### SSL Parameters

Enable DH Param  
Refresh Count  
  
File Path\*  
  ▼ ?

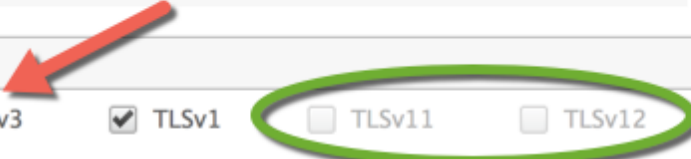
Enable Ephemeral RSA  
 Enable Session Reuse  
Time-out

Enable Cipher Redirect  
 SSLv2 Redirect  
 Client Authentication

SSL Redirect  
 SNI Enable  
 Send Close-Notify  
Clear Text Port  
  
PUSH Encryption Trigger  
 ▼

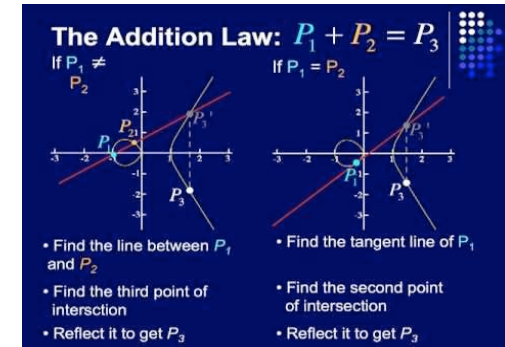
### Protocol

SSLv2  SSLv3  TLSv1  TLSv11  TLSv12



# Change Cipher Suites

Better on the CLI – some GUI issues on actual build



## Create custom cipher group

- add ssl cipher YOUR-DEFAULT-ECCPFS
- bind ssl cipher YOUR-DEFAULT-ECCPFS -cipherName TLS1-ECDHE-RSA-AES256-SHA
- bind ssl cipher YOUR-DEFAULT-ECCPFS -cipherName TLS1-DHE-RSA-AES-256-CBC-SHA
- bind ssl cipher YOUR-DEFAULT-ECCPFS -cipherName TLS1-AES-256-CBC-SHA

## Bind custom cipher group to SSL Vserver

- bind ssl vserver <vserverName> -cipherName YOUR-DEFAULT-ECCPFS

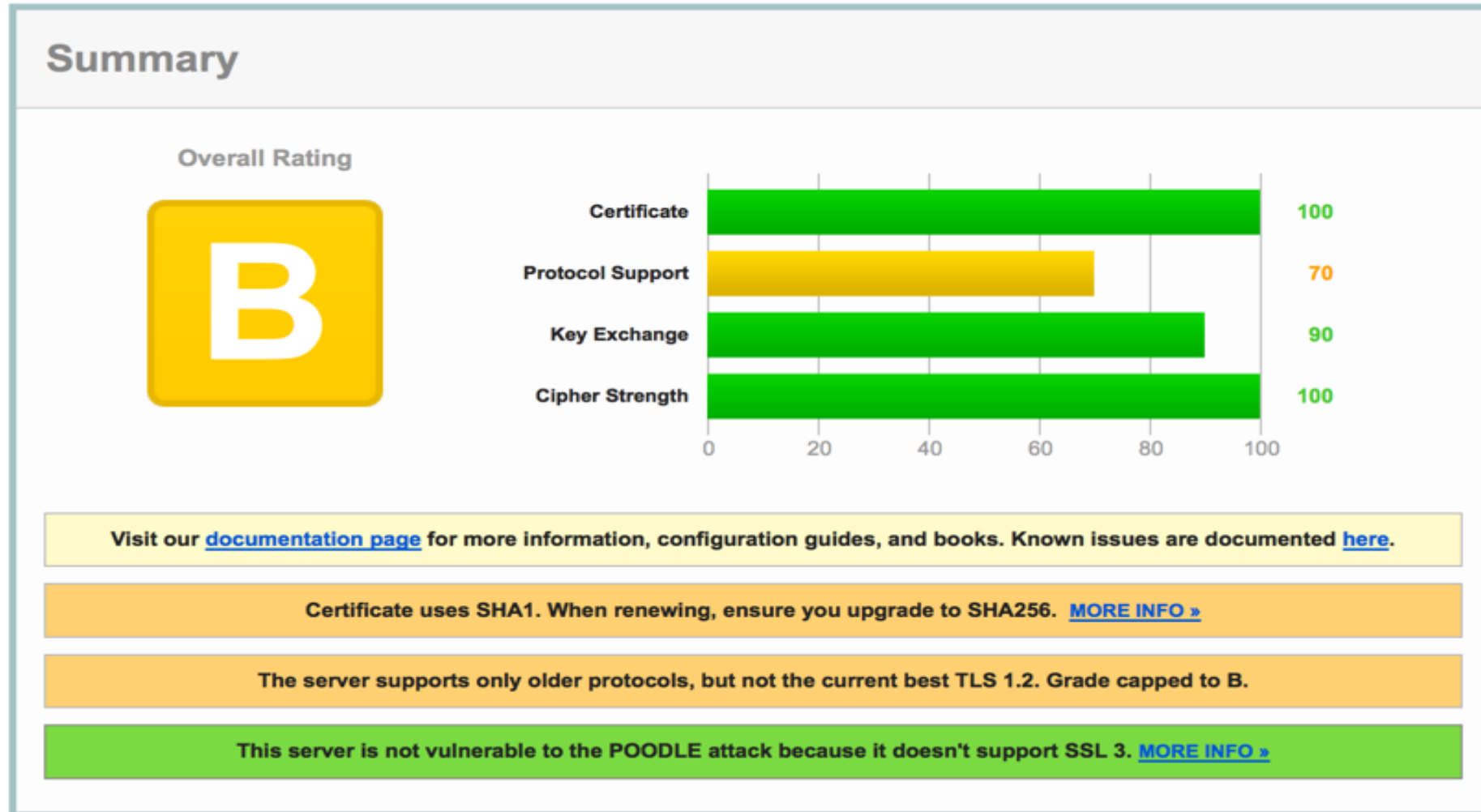
## Bind ECC curves to SSL Vserver

- bind ssl vserver <vserverName> -eccCurveName ALL  
(Only on VPX and MPX/SDX115xx and higher)



| Symmetric Key Size (bits) | RSA and Diffie-Hellman Key Size (bits) | Elliptic Curve Key Size (bits) |
|---------------------------|--|--------------------------------|
| 80                        | 1024                                   | 160                            |
| 112                       | 2048                                   | 224                            |
| 128                       | 3072                                   | 256                            |
| 192                       | 7680                                   | 384                            |
| 256                       | 15360                                  | 521                            |

Table 1: NIST Recommended Key Sizes


# Better SSL Rating (on non VPX A+)



# Just the Ciphers we want

| Configuration  |  |
|--|--|
|   | <b>Protocols</b>   |
|  | <hr/>  |
|  | <b>TLS 1.2</b> <span style="float: right;">No</span>   |
|  | TLS 1.1 <span style="float: right;">No</span>  |
|  | TLS 1.0 <span style="float: right;">Yes</span>   |
|  | SSL 3 <span style="float: right;">No</span>  |
|  | SSL 2 <span style="float: right;">No</span>  |
|  | <hr/>  |
|  | <b>Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites always at the end)</b>            |
|  | <hr/>  |
|  | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH 256 bits (eq. 3072 bits RSA) FS <span style="float: right;">256</span>  |
|  | TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0xc039) DH 2048 bits (p: 256, g: 1, Ys: 256) FS <span style="float: right;">256</span> |
|  | TLS_RSA_WITH_AES_256_CBC_SHA (0xc035) <span style="float: right;">256</span>   |
|  | <hr/>  |

# Forward Secrecy on all supported platforms



| Handshake Simulation                         |  |                                   |   |    |                   |
|--|--|-----------------------------------|---|----|-------------------|
| <a href="#">Android 2.3.7</a>                | No SNI <sup>2</sup>                    | Protocol or cipher suite mismatch |   |    | Fail <sup>3</sup> |
| <a href="#">Android 4.0.4</a>                |  | TLS 1.0                           | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | FS | 256               |
| <a href="#">Android 4.1.1</a>                |  | TLS 1.0                           | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | FS | 256               |
| <a href="#">Android 4.2.2</a>                |  | TLS 1.0                           | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | FS | 256               |
| <a href="#">Android 4.3</a>                  |  | TLS 1.0                           | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | FS | 256               |
| <a href="#">Android 4.4.2</a>                |  | TLS 1.0                           | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | FS | 256               |
| <a href="#">BingBot Dec 2013</a>             | No SNI <sup>2</sup>                    | TLS 1.0                           | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | FS | 256               |
| <a href="#">BingPreview Jun 2014</a>         |  | TLS 1.0                           | TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)     | FS | 256               |
| <a href="#">Chrome 37 / OS X</a>             | R                                      | TLS 1.0                           | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | FS | 256               |
| <a href="#">Firefox 24.2.0 ESR / Win 7</a>   |  | TLS 1.0                           | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | FS | 256               |
| <a href="#">Firefox 32 / OS X</a>            | R                                      | TLS 1.0                           | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | FS | 256               |
| <a href="#">Googlebot Jun 2014</a>           |  | TLS 1.0                           | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | FS | 256               |
| <a href="#">IE 6 / XP</a>                    | No FS <sup>1</sup> No SNI <sup>2</sup> | Protocol or cipher suite mismatch |   |    | Fail <sup>3</sup> |
| <a href="#">IE 7 / Vista</a>                 |  | TLS 1.0                           | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | FS | 256               |
| <a href="#">IE 8 / XP</a>                    | No FS <sup>1</sup> No SNI <sup>2</sup> | Protocol or cipher suite mismatch |   |    | Fail <sup>3</sup> |
| <a href="#">IE 8-10 / Win 7</a>              | R                                      | TLS 1.0                           | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | FS | 256               |
| <a href="#">IE 11 / Win 7</a>                | R                                      | TLS 1.0                           | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | FS | 256               |
| <a href="#">IE 11 / Win 8.1</a>              | R                                      | TLS 1.0                           | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | FS | 256               |
| <a href="#">IE Mobile 10 / Win Phone 8.0</a> |  | TLS 1.0                           | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | FS | 256               |
| <a href="#">IE Mobile 11 / Win Phone 8.1</a> |  | TLS 1.0                           | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | FS | 256               |

# Network Tracing

# Technical Preparation:

Certificates: **XenMobile** Server-side



**Public Certificates:** Obtain the two individual certs needed to support:

- **XenMobile MDM:** cert *tied to the MDM FQDN* – secures the trusted MDM enrollment of devices and allows for SSO capabilities later.
- **XenMobile MAM:** cert *tied to the NetScaler Gateway FQDN* for the **XenMobile WorxHome & WorxStore** access, and (mVPN) services required for the secure tunneling of Worx enabled apps.
- **NOTE:** *Individual named certs recommended. Use of Wildcard “\*.domain.com” certs are okay, but SAN-certs are not compatible.*

# SSL Certificates

## Helpful tools

### OpenSSL

```
# Generate a 2048-bit private key
openssl genrsa -out my.key 2048
# Create a Certificate Signing Request
openssl req -new -key my.key -out my.csr
# Create a self-signed certificate with a 365-day expiration
openssl x509 -req -days 365 -in my.csr -signkey my.key -out my.crt
# Convert a Certificate from DER to PEM
openssl x509 -inform der -in certificate.cer -out certificate.pem
# Convert a Certificate from PEM to PFX
openssl pkcs12 -export -out cert.pfx -inkey priv.key -in cert.crt -certfile CACert.crt
```



# SSL Certificates

Helpful tools

## XCA Certificate and key managements – CSR, KEY, CERT DB

The screenshot shows the XCA Certificate and Key management application window. The 'Certificates' tab is active, displaying a list of certificates with columns for Internal name, commonName, CA, and Serial. The list includes various certificates from LLV Issuing CA, SwissSign, Symantec, and Thawte. A sidebar on the right contains buttons for 'New Certificate', 'Export', 'Import', 'Show Details', 'Delete', 'Import PKCS#12', 'Import PKCS#7', and 'Plain View'. At the bottom left, the database path is shown as '/Users/danielk/Documents/daniel.xdb'.

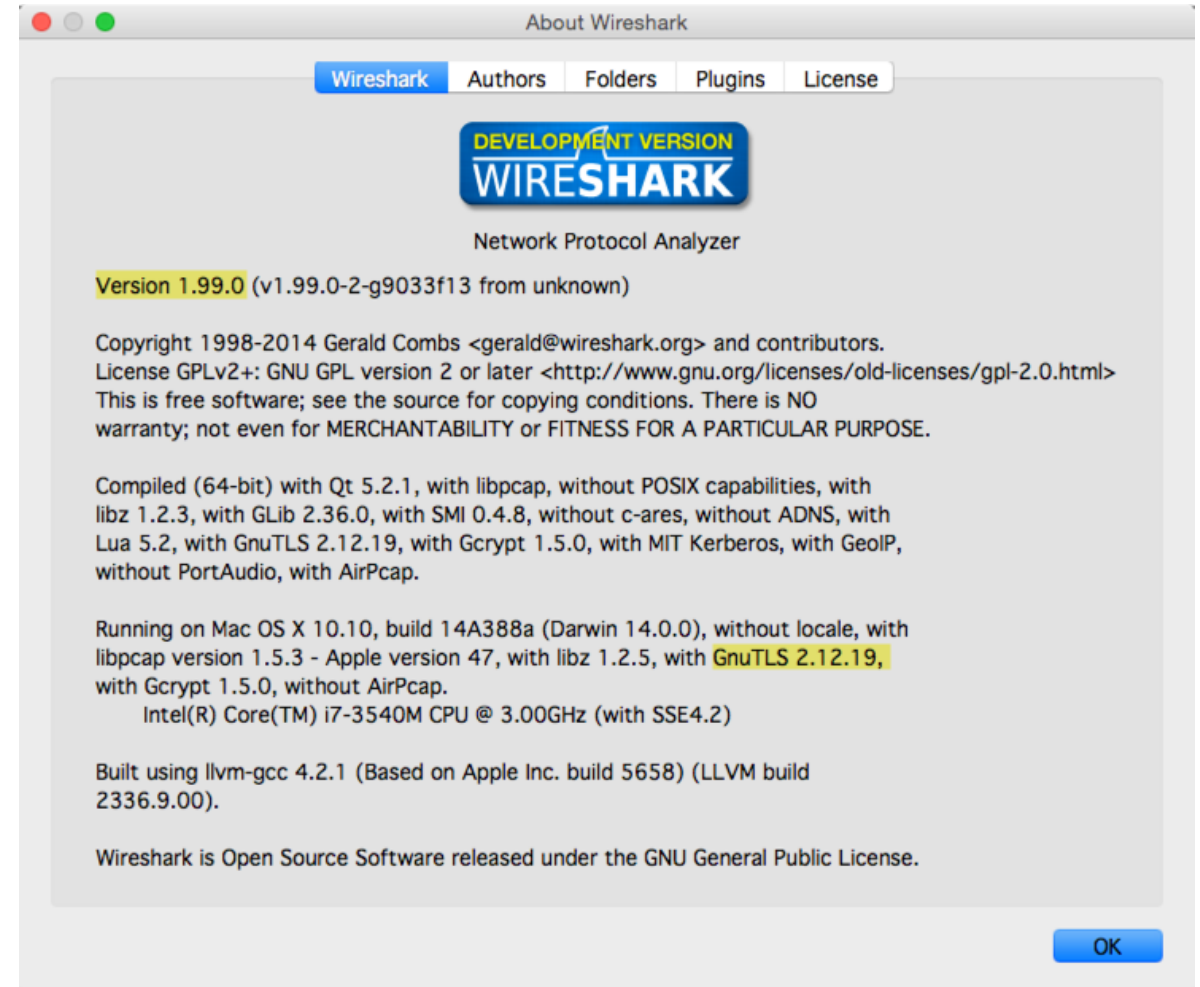
| Internal name                                 | commonName                                    | CA  | Serial                     |
|---|---|-----|----------------------------|
| LLV Issuing CA General                        | LLV Issuing CA General                        | Yes | 1101AB800000i              |
| SwissSign Silver CA – G2                      | SwissSign Silver CA – G2                      | Yes | 4F1BD42F5                  |
| SwissSign Server Silver CA 2008 – G2          | SwissSign Server Silver CA 2008 – G2          | 0   | 9D154E306i                 |
| intportal.fma-li.li                           | intportal.fma-li.li                           |     | B2611E101AEABDA79D4956B    |
| mwst.llv.li                                   | mwst.llv.li                                   |     | ACD80CD61BA2685DD35657E    |
| testportal.fma-li.li                          | testportal.fma-li.li                          |     | 6061BA42D2A6271E05EB1DD    |
| www.llv.li                                    | www.llv.li                                    |     | CAB25A2808BB4BB50F9421E    |
| www.portal.fma-li.li                          | www.portal.fma-li.li                          |     | 18563B9204505309986129E    |
| Symantec Enterprise Mobile Root for Micros... | Symantec Enterprise Mobile Root for Microsoft | Yes | 0F6B552F9EBF907B0F6629A9B1 |
| Symantec Enterprise Mobile CA for Mcro...     | Symantec Enterprise Mobile CA for Microsoft   | 0   | 25E719F028FF1B1E1D2797B99  |
| AXACOM AG                                     | AXACOM AG                                     | No  |                            |
| Citrix  | Citrix  | No  |                            |
| UTN – DATACorp SGC                            | UTN – DATACorp SGC                            | Yes | 46EAF096054CC5E3FA65EA6E5  |
| COMODO Certification Authority                | COMODO Certification Authority                | Yes | 2E79832E908887EA8B8EF31A6  |
| EssentialSSL CA                               | EssentialSSL CA                               | 0   | 18B2CBBAA304F1A00FC1F2F3E  |
| thawte Primary Root CA                        | thawte Primary Root CA                        | Yes | 344ED55720D5EDEC49F42FCE3  |
| Thawte SSL CA                                 | Thawte SSL CA                                 | 0   | 4D5F2C3408B24C20CD6D507E2  |
| *.opo.ch                                      | *.opo.ch                                      | No  | 046435F003F8230A3212D13A7  |
| formulare.llv.li                              | formulare.llv.li                              | No  | 5C4AF824C7B860A770A6DFA5E7 |
| my.schaeppli.ch                               | my.schaeppli.ch                               | No  | 2F71C77CE1F1213C9B2138EB2  |

# Troubleshooting

## Using Wireshark

Able to capture, decrypt and decode SSL traffic if

- Captured on a Ethernet tap or shared media hub
- Wireshark can capture in promiscuous mode
- Wireshark is compiled with GnuTLS support
- RSA key is accessible
- Port, Protocol and SSL Server IP address is configured



# Troubleshooting

## Options for capturing packets

### No access to (shared) network

- Install Wireshark or tcpdump locally on each server
- Capture packets on the Netscaler (Choose tcpdump or nstrace format)

#### Technical Support Tools

[Generate support file](#)

[Start new trace](#)

[Download trace files](#)

[Download core files](#)

[Get back trace](#)

[Call Home](#)

### Trace

**Packet Size**  
164

Duration of data per file (seconds)  
3600

Enable TCP dump for .pcap file format

Number of trace files  
24

Trace file name

Trace File ID

Trace Buffers  
5000

Filter Expression  
Operators Saved Policy Expressions Frequently Used Expressions

Press Control+Space to start the expression and then type '.' to get the next set of options

Trace filtered connection's peer traffic  Do Runtime merge  
 Do Runtime cleanup  Skip RPC

#### Capturing Mode

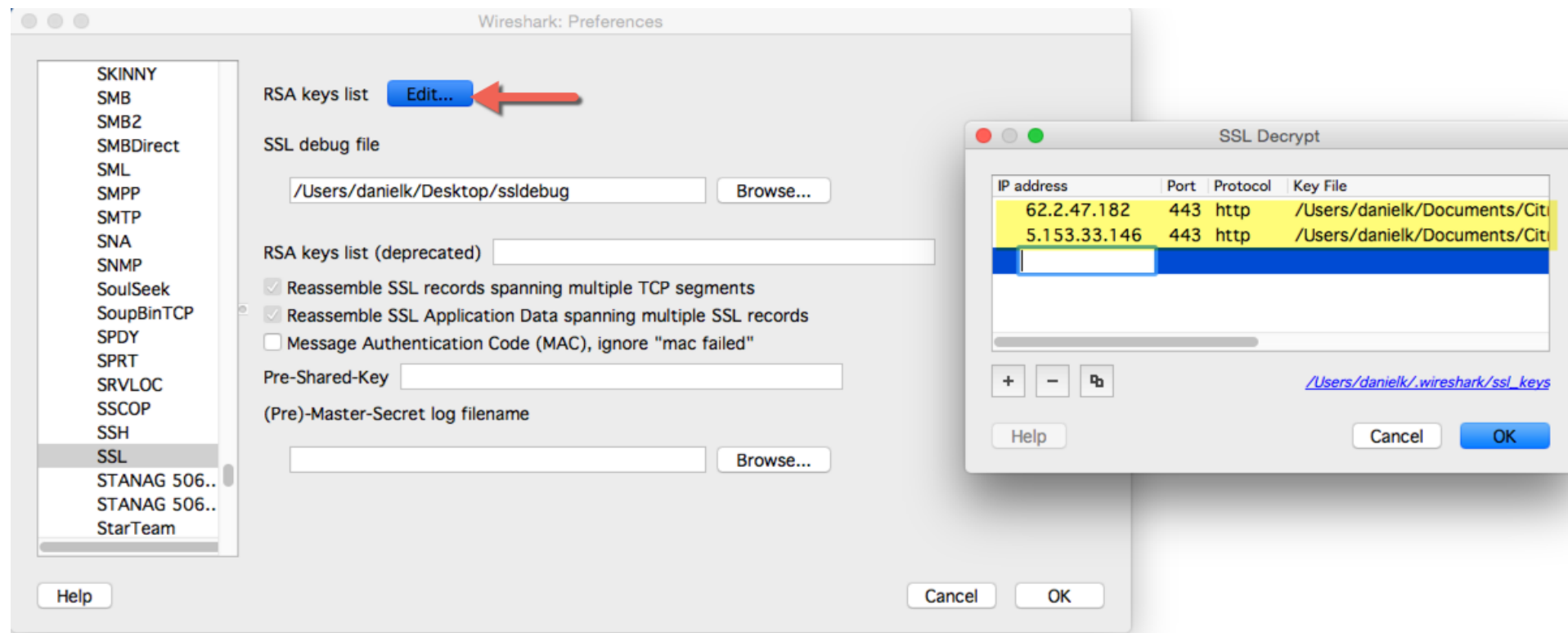
Packets buffered for transmission  Transmitted packets  
 Received packets before NIC pipelining  Received packets after NIC pipelining  
 Translated IPV6 packets  Packets are not captured in flow receiver  
 Capture C2C message

**Start** **Close**

# Troubleshooting

## Using Wireshark

Configure Wireshark for SSL decryption  
Preferences -> Protocols -> SSL



# Troubleshooting

## Using Wireshark

### DH Keys can't be used to decipher SSL traffic

- Consider SSL Offload with the NetScaler and check the ciphers (RSA only)

Handshake packets point to Diffie Hellman

| No. | Time        | Source          | Destination     | Protocol | Length | Info   |
|-----|-------------|-----------------|-----------------|----------|--------|--|
| 7   | 0.110848000 | 77.57.187.121   | 178.197.225.233 | TCP      | 1434   | [TCP segment of a reassembled PDU]   |
| 8   | 0.110969000 | 77.57.187.121   | 178.197.225.233 | TLSv1.2  | 1152   | Server Hello, Certificate, Server Key Exchange, Server Hello Done                |
| 9   | 0.149957000 | 178.197.225.233 | 77.57.187.121   | TCP      | 66     | 39217-8443 [ACK] Seq=183 Ack=4105 Win=131072 Len=0 TSval=260922946 TSecr=2436868 |
| 10  | 0.158022000 | 178.197.225.233 | 77.57.187.121   | TCP      | 66     | 39217-8443 [ACK] Seq=183 Ack=5191 Win=129984 Len=0 TSval=260922947 TSecr=2436868 |
| 11  | 0.228377000 | 178.197.225.233 | 77.57.187.121   | TLSv1.2  | 1152   | Client Key Exchange  |
| 12  | 0.228377000 | 178.197.225.233 | 77.57.187.121   | TLSv1.2  | 72     | Change Cipher Spec   |
| 13  | 0.229188000 | 178.197.225.233 | 77.57.187.121   | TLSv1.2  | 167    | Encrypted Handshake Message  |
| 14  | 0.229151000 | 77.57.187.121   | 178.197.225.233 | TCP      | 66     | 8443-39217 [ACK] Seq=5191 Ack=264 Win=65536 Len=0 TSval=2436880 TSecr=260922996  |
| 15  | 0.235322000 | 77.57.187.121   | 178.197.225.233 | TLSv1.2  | 72     | Change Cipher Spec   |
| 16  | 0.235366000 | 77.57.187.121   | 178.197.225.233 | TLSv1.2  | 167    | Encrypted Handshake Message  |
| 17  | 0.269970000 | 178.197.225.233 | 77.57.187.121   | TCP      | 66     | 39217-8443 [ACK] Seq=365 Ack=5197 Win=131056 Len=0 TSval=260923063 TSecr=2436881 |

Application Data: Meaningless data string

| No. | Time        | Source          | Destination     | Protocol | Length | Info  |
|-----|-------------|-----------------|-----------------|----------|--------|---|
| 19  | 0.281206000 | 178.197.225.233 | 77.57.187.121   | TLSv1.2  | 407    | Application Data  |
| 20  | 0.366592000 | 77.57.187.121   | 178.197.225.233 | TLSv1.2  | 359    | Application Data  |
| 21  | 0.366636000 | 77.57.187.121   | 178.197.225.233 | TLSv1.2  | 519    | Application Data  |
| 22  | 0.430048000 | 178.197.225.233 | 77.57.187.121   | TCP      | 66     | 39217-8443 [ACK] Seq=706 Ack=5591 Win=130768 Len=0 TSval=260923218 TSecr=2436894  |
| 23  | 0.437746000 | 178.197.225.233 | 77.57.187.121   | TCP      | 66     | 39217-8443 [ACK] Seq=706 Ack=6044 Win=130320 Len=0 TSval=260923218 TSecr=2436894  |
| 24  | 1.660251000 | 178.197.225.233 | 77.57.187.121   | TLSv1.2  | 407    | Application Data  |
| 25  | 1.669722000 | 77.57.187.121   | 178.197.225.233 | TLSv1.2  | 359    | Application Data  |
| 26  | 1.669960000 | 77.57.187.121   | 178.197.225.233 | TLSv1.2  | 327    | Application Data  |
| 27  | 1.710067000 | 178.197.225.233 | 77.57.187.121   | TCP      | 66     | 39217-8443 [ACK] Seq=1047 Ack=6337 Win=130768 Len=0 TSval=260924493 TSecr=2437024 |
| 28  | 1.717740000 | 178.197.225.233 | 77.57.187.121   | TCP      | 66     | 39217-8443 [ACK] Seq=1047 Ack=6598 Win=130512 Len=0 TSval=260924493 TSecr=2437024 |
| 29  | 1.759250000 | 178.197.225.233 | 77.57.187.121   | TLSv1.2  | 407    | Application Data  |

# Troubleshooting

## Using Wireshark

Providing the RSA key, server ip and port number allows Wireshark to decrypt and decode SSL

Filter: `(ip.addr eq 178.197.225.233 and ip.addr eq 217.162.78.130)`

| No. | Time         | Source          | Destination     | Protocol | Length | Info  |
|-----|--------------|-----------------|-----------------|----------|--------|---|
| 799 | 58.028895000 | 178.197.225.233 | 217.162.78.130  | TCP      | 78     | 17368-443 [SYN] Seq=0 Win=65535 Len=0 MSS=1380 WS=16 TSval=260980459 TSecr=0 SACK...  |
| 802 | 58.030288000 | 217.162.78.130  | 178.197.225.233 | TCP      | 60     | 443-17368 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1360                              |
| 808 | 58.061719000 | 178.197.225.233 | 217.162.78.130  | TCP      | 60     | 17368-443 [ACK] Seq=1 Ack=1 Win=1048560 Len=0   |
| 815 | 58.086684000 | 178.197.225.233 | 217.162.78.130  | TLSv1    | 267    | Client Hello  |
| 816 | 58.088155000 | 217.162.78.130  | 178.197.225.233 | TLSv1    | 183    | Server Hello, Change Cipher Spec, Finished  |
| 829 | 58.139763000 | 178.197.225.233 | 217.162.78.130  | TCP      | 60     | 17368-443 [ACK] Seq=214 Ack=130 Win=1048560 Len=0                                     |
| 830 | 58.139805000 | 178.197.225.233 | 217.162.78.130  | TLSv1    | 60     | Change Cipher Spec  |
| 832 | 58.139851000 | 178.197.225.233 | 217.162.78.130  | TLSv1    | 91     | Finished  |
| 833 | 58.141045000 | 217.162.78.130  | 178.197.225.233 | TCP      | 60     | 443-17368 [ACK] Seq=130 Ack=220 Win=35256 Len=0                                       |
| 834 | 58.141149000 | 217.162.78.130  | 178.197.225.233 | TCP      | 60     | 443-17368 [ACK] Seq=130 Ack=257 Win=35219 Len=0                                       |
| 836 | 58.141807000 | 178.197.225.233 | 217.162.78.130  | HTTP     | 728    | GET /cvpn/https/ac2.hol.local/Citrix/Store/resources/v2/0zE1NzUyMzI2Njc3RDJC0EMIRT... |

Handshake packets point to RSA

Filter: `(ip.addr eq 178.197.225.233 and ip.addr eq 217.162.78.130)`

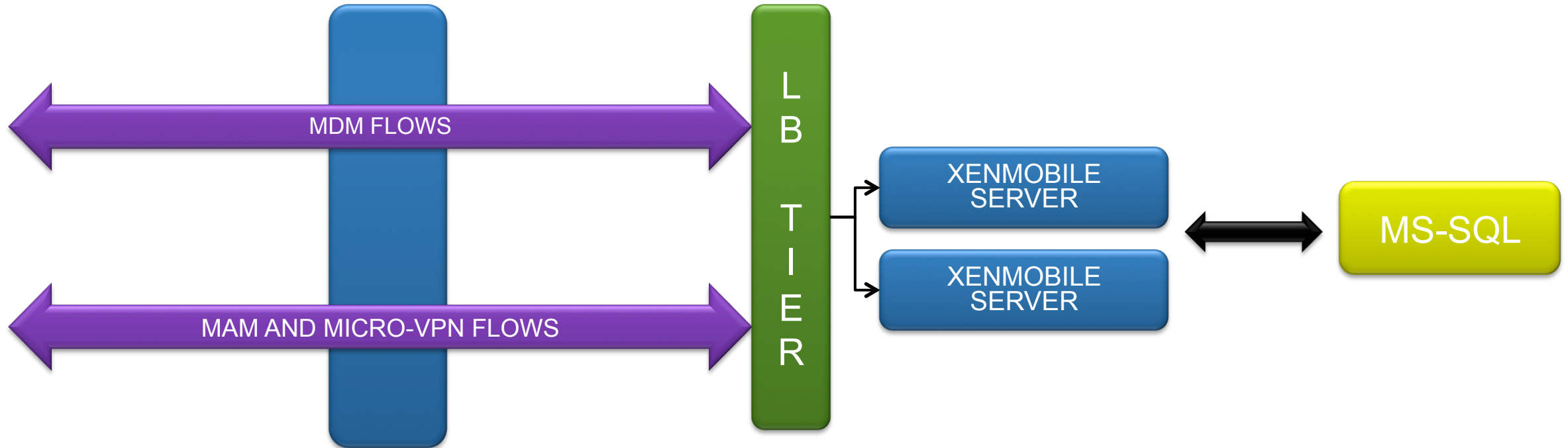
| No. | Time         | Source          | Destination     | Protocol | Length | Info  |
|-----|--------------|-----------------|-----------------|----------|--------|---|
| 836 | 58.141807000 | 178.197.225.233 | 217.162.78.130  | HTTP     | 728    | GET /cvpn/https/ac2.hol.local/Citrix/Store/resources/v2/0zE1NzUyMzI2Njc3RDJC0EMIRT... |
| 847 | 58.160788000 | 217.162.78.130  | 178.197.225.233 | TLSv1    | 165    | [SSL segment of a reassembled PDU]  |
| 848 | 58.162408000 | 217.162.78.130  | 178.197.225.233 | TCP      | 4134   | [TCP segment of a reassembled PDU]  |
| 849 | 58.162612000 | 217.162.78.130  | 178.197.225.233 | HTTP     | 1807   | HTTP/1.1 200 OK (PNG)   |

Decoded as clear text HTTP

# Titan - Preview

## ACCESS TIER

## XM-TITAN ARCHITECTURE



Single unified « XENMOBILE SERVER » with all device and app management features

Unified administrative console with AD integration, and RBAC support

External data store, for simpler scalability, HA, DR and multi-site rollout

Consolidated logging, reporting and event management



# XenMobile Titan – Platform Review

## Active Directory

- LDAP and LDAPS
- Multi-domain
- Global Catalog support
- On-demand AD (No sync, delta sync etc)
- No first-name, last-name dependency
- Sync required for “Nested Groups” support - Optional

## DB

- MS SQL 2012+
- DR with DB replication

## PKI

- No change from XM9
  - MSFT CA for user certs

## Syslog

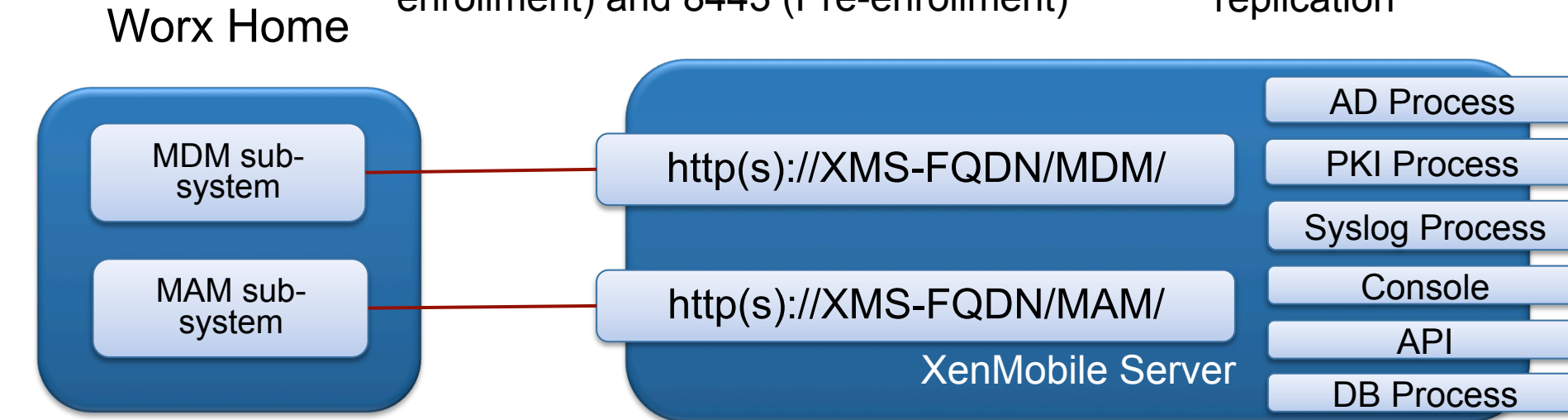
- Unified logging
- User activity
- Admin activity
- System activity

## MDM Endpoint Interface

- Listening on ports 443 (Cert based post-enrollment) and 8443 (Pre-enrollment)

## MAM Endpoint Interface

- Listening on ports 443 (non-cert based)



## Unified console

- RBAC for MDM and MAM configuration
- AD user as admin
- Local user creation for MDM/ MAM enrollments

## API

- Carryover of XDM API
- Backwards compatible
- NOTE: No MAM config APIs

# Unified Administrative Console

The screenshot displays the XenMobile Unified Administrative Console interface. The browser address bar shows the URL [https://xm2.mpg.citrix.com/index\\_uc.html#](https://xm2.mpg.citrix.com/index_uc.html#). The navigation menu includes **Dashboard**, **Manage**, and **Configure** (highlighted). The main content area is divided into **Devices** and **Policies** sections.

**Devices** section:

- Buttons: Add, Import
- Table columns: Status, Type, Created On, Last Updated On, Status
- Showing 1 to 2 of 2

**Policies** section:

- Buttons: Add
- Search bar: Search
- Table columns: Policy Name, Type, Created On, Last Updated On, Status
- Message: No results found.

The left sidebar contains sections for **NOTIFICATIONS**, **PLATFORMS**, and **MANAGED DEVICES**.

