Citrix XenMobile Enterprise Edition

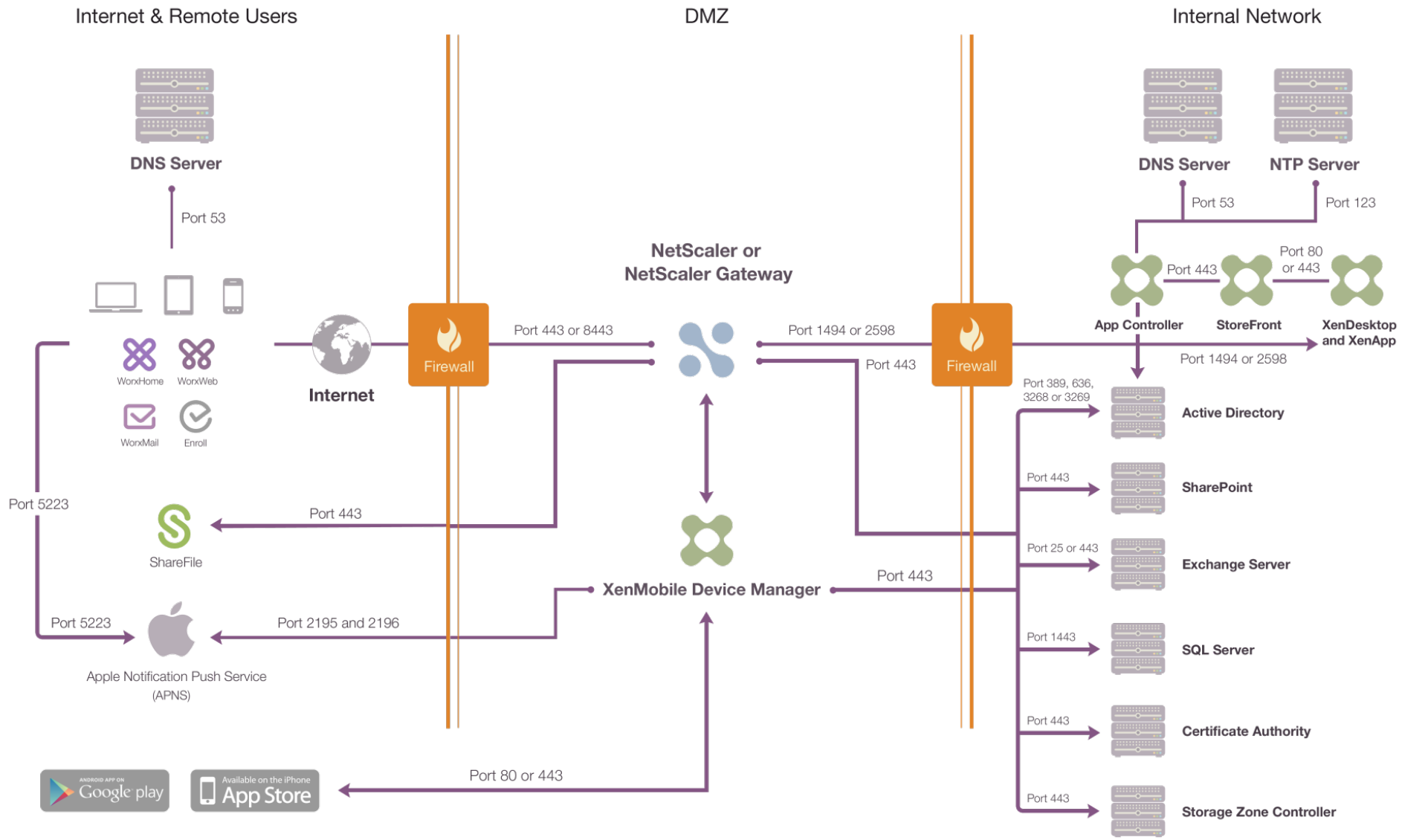
Claudio Mascaro
Senior Systems Engineer
BCD-Sintrag AG

Daniel Kuenzli
Senior Systems Engineer
Citrix Systems GmbH

EMM

Enterprise Mobility 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

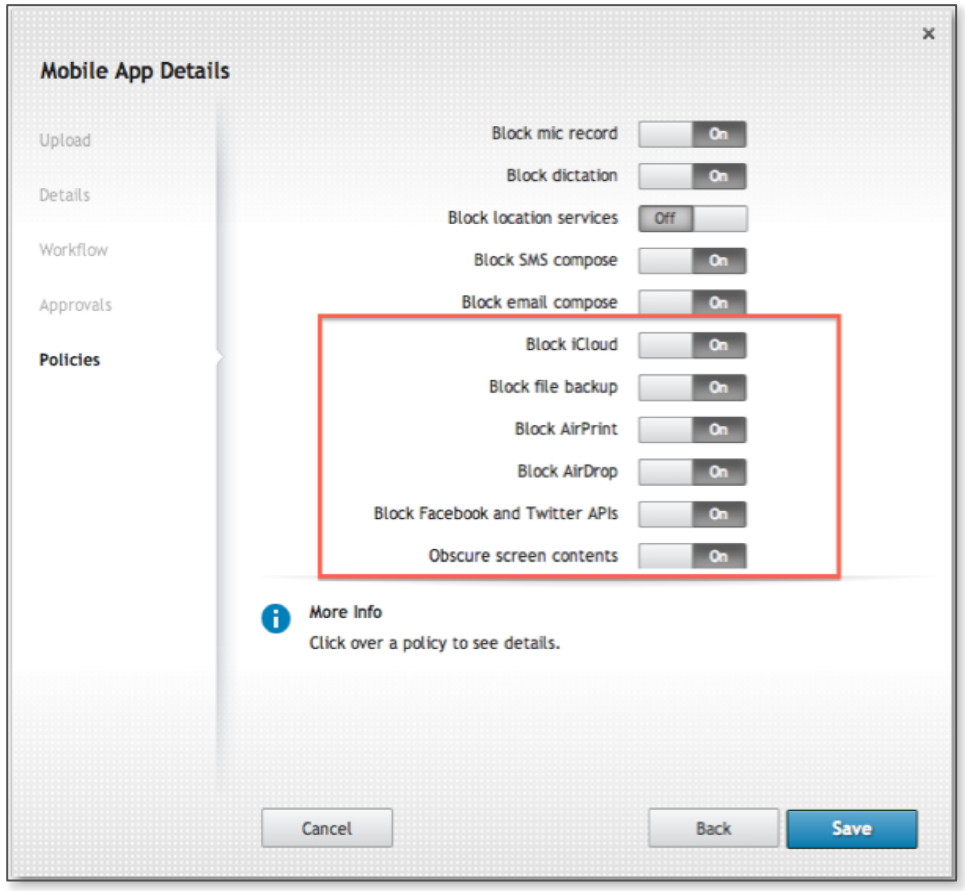
WorxDesktop

- 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

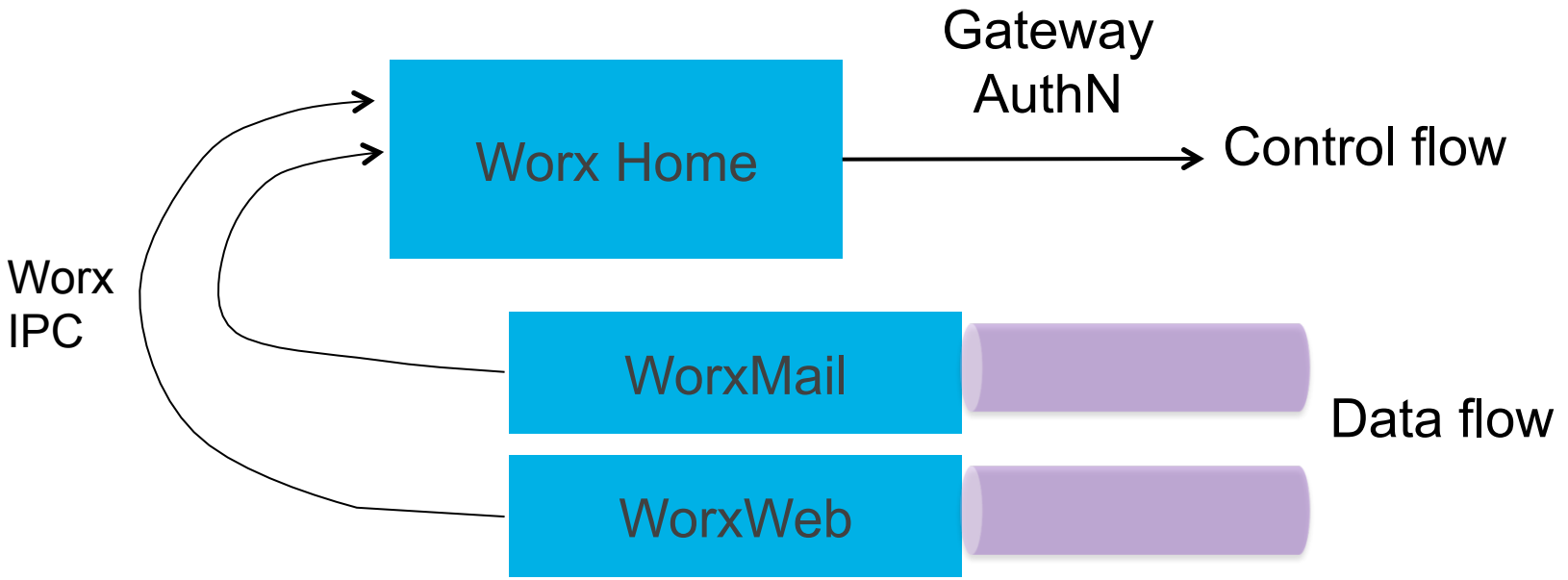
- XenMobile generated OTP for MDM enrollment
- RADIUS OTP support for MAM authentication

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)

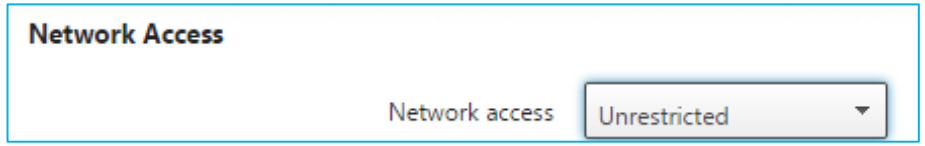
WorxWeb Einsatzszenarien

Infrastruktur

XenMobile App Controller

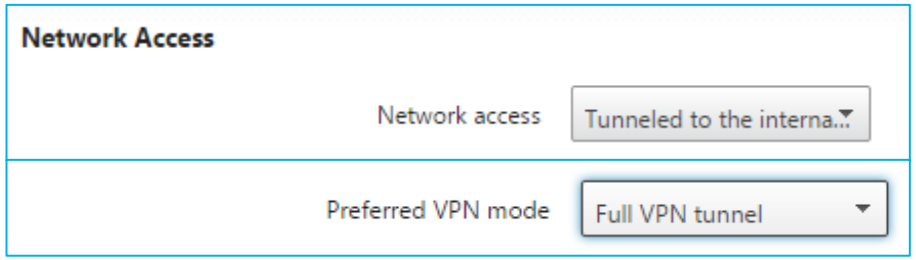
WorxWeb direkt zu WebServer

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



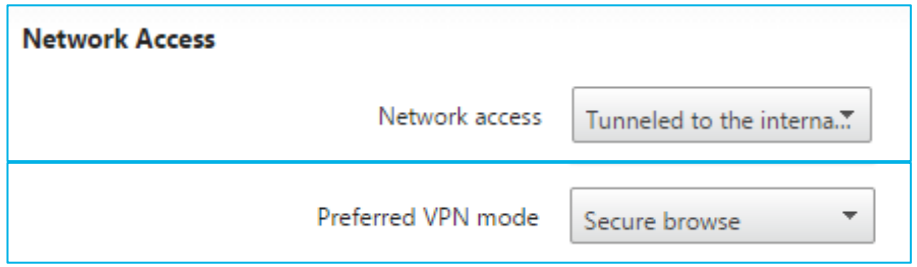
WorxWeb mit mVPN Tunnel

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

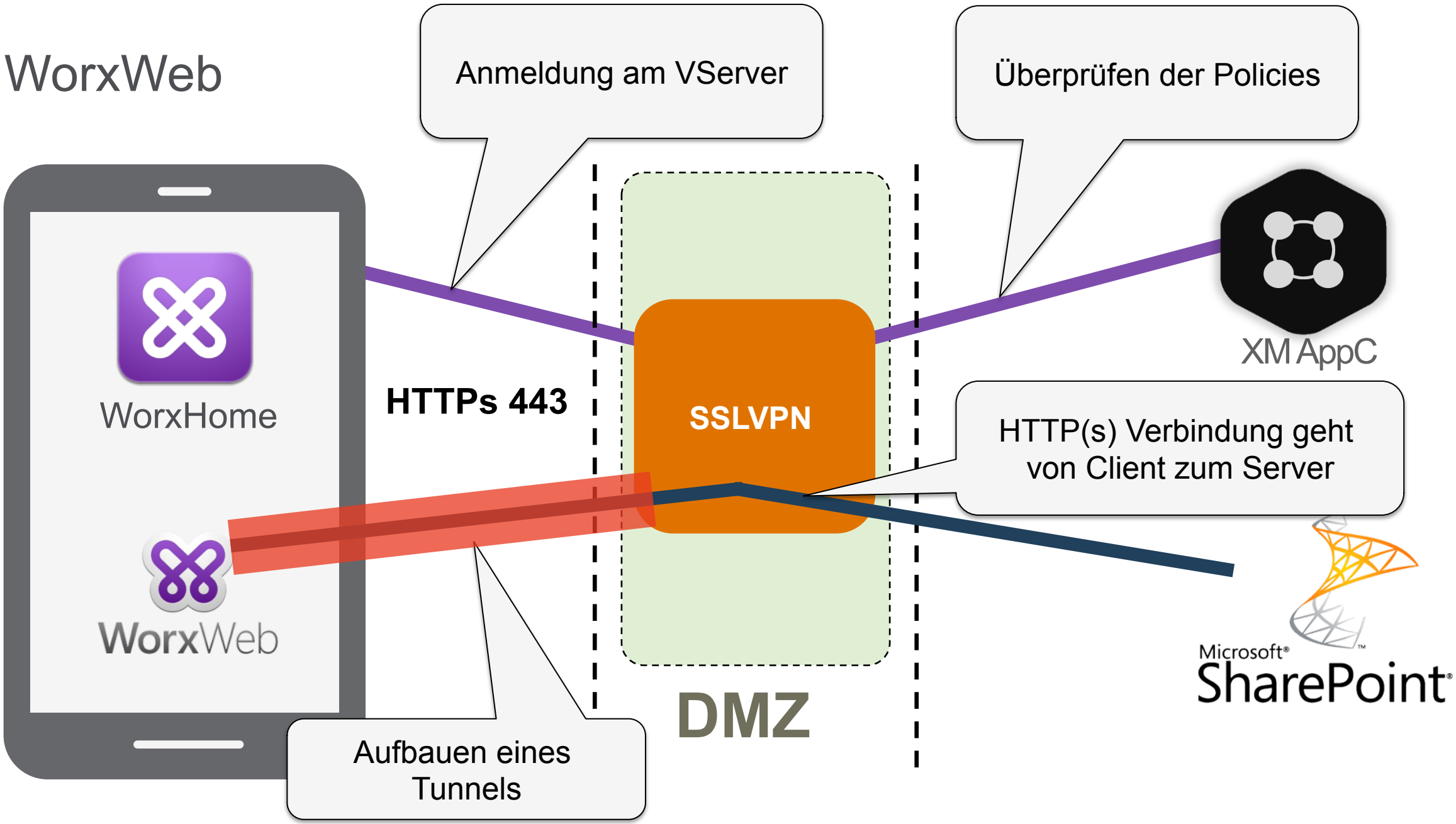


WorxWeb mit SecureBrowse

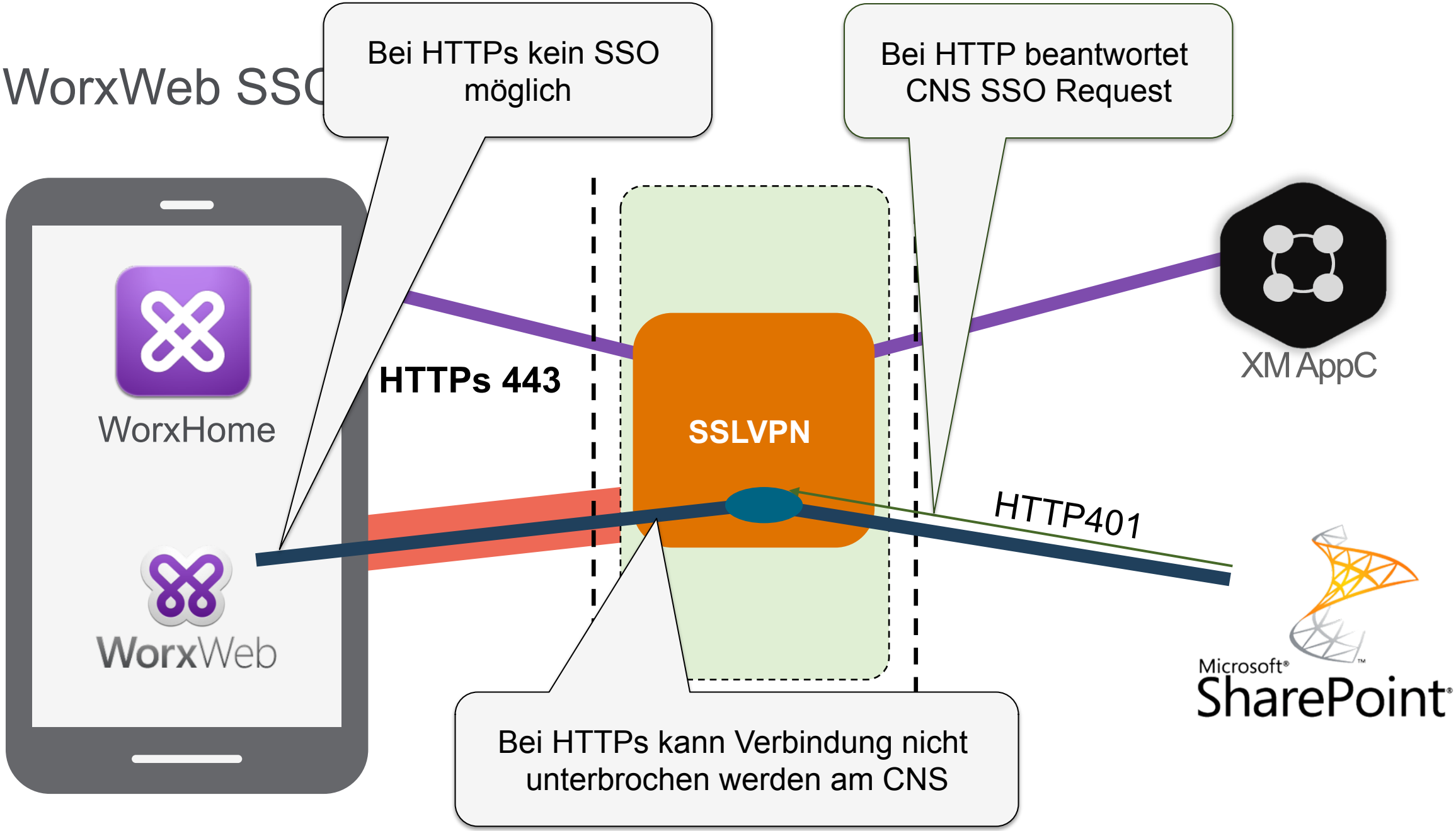
- Umschreiben am Client (Aufwand)
- SSO auch für HTTPs möglich



WorxWeb



WorxWeb SSO



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

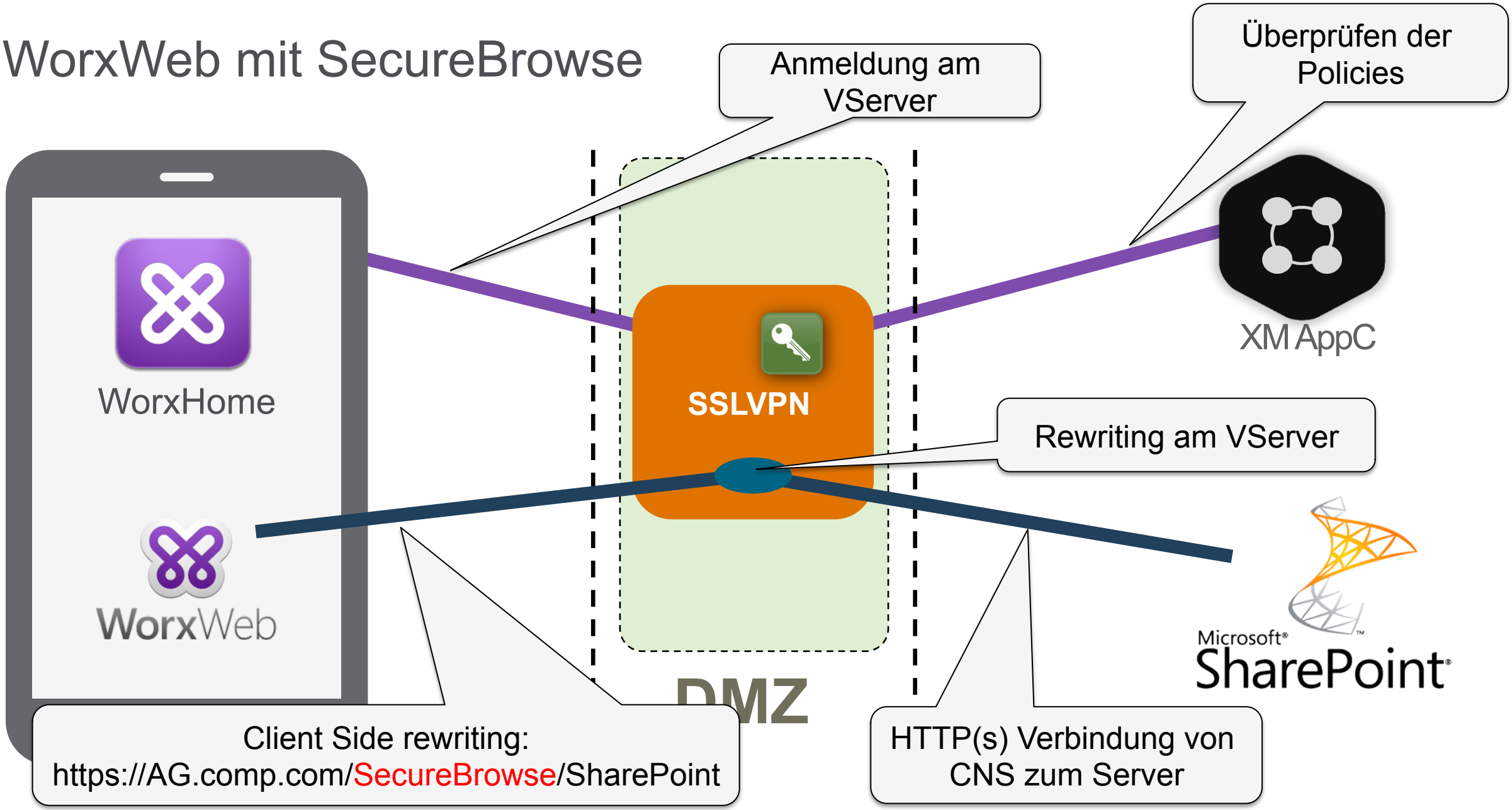
NetScaler ist aus Sicht des WebServers der Client (SSL Verbindung)

NetScaler kann für HTTP und HTTPs SSO Requests beantworten

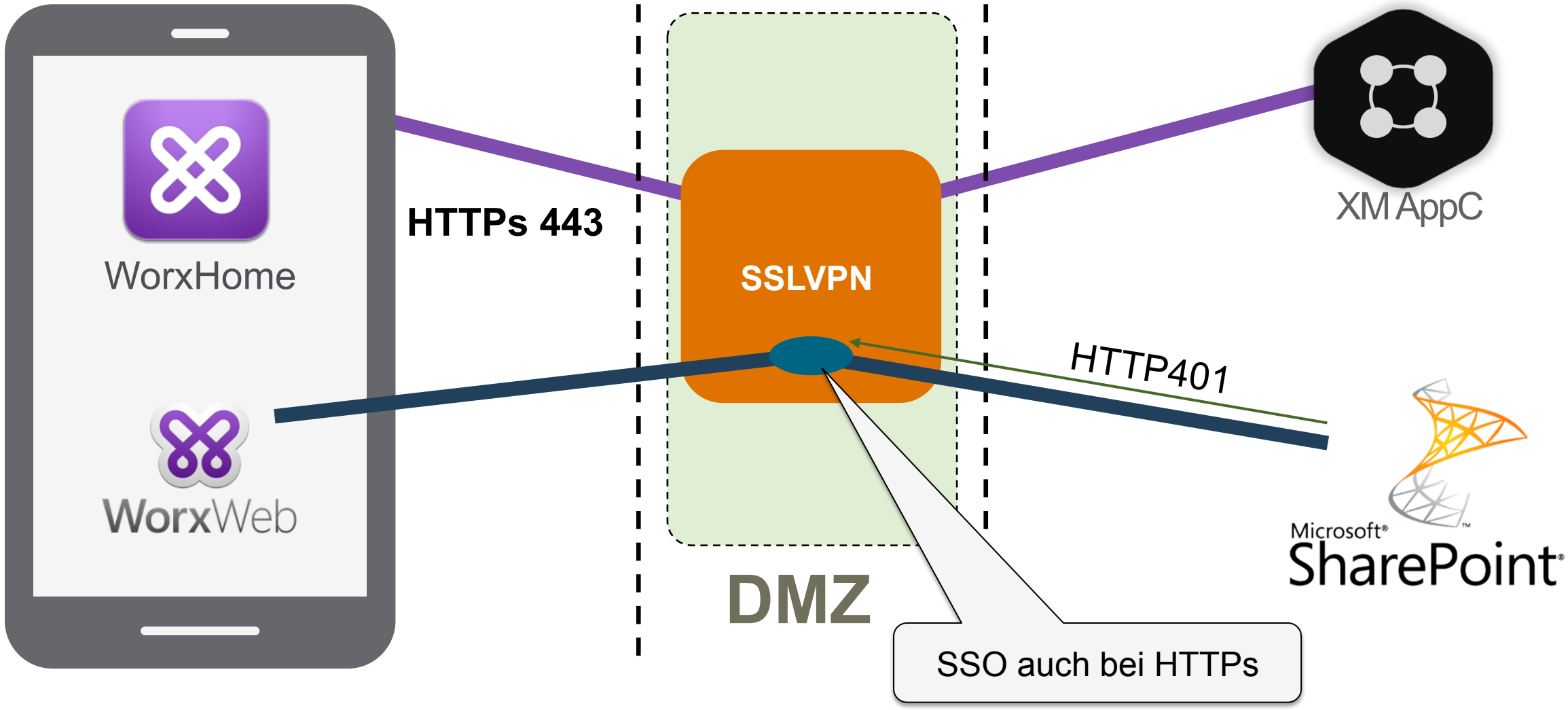
Mehr Rechenaufwand am Browser und am NetScaler als mVPN

Es wird keinTunnel *offen* gehalten

WorxWeb mit SecureBrowse

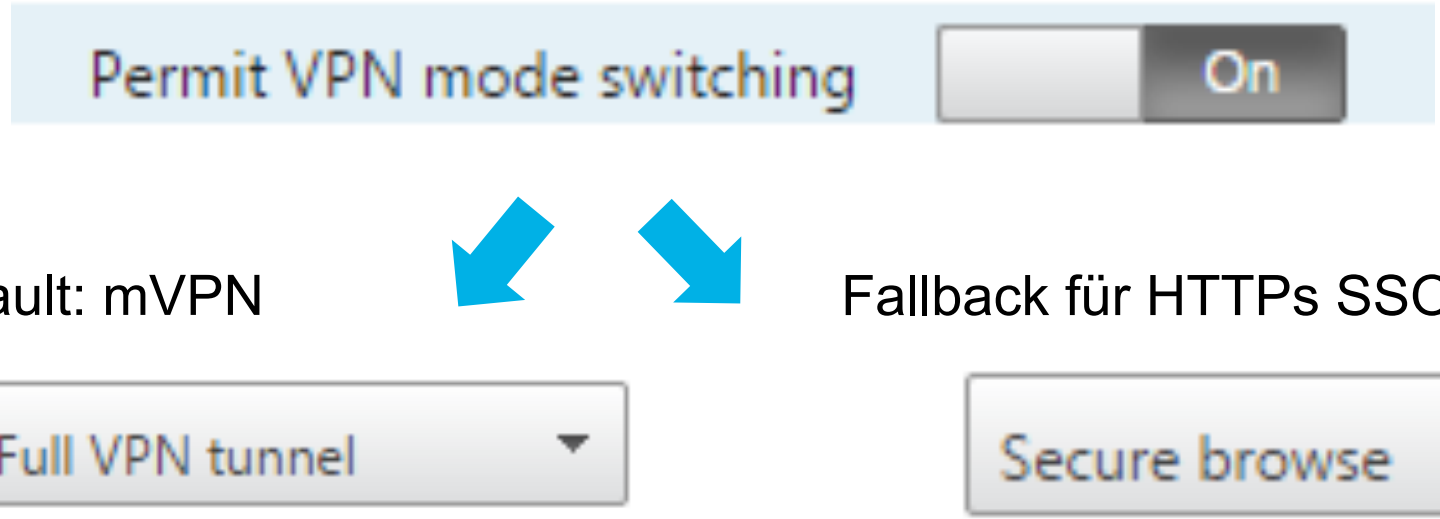


WorxWeb mit SecureBrowse



WorxWeb: MicroVPN Flexibility

Permit VPN mode switching



Beispiele für HTTP Proxy Traffic Policies (non global)

Internes WiFi Netz

- Int**er**net Daten gehen über Proxy Server
- Int**ra**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:

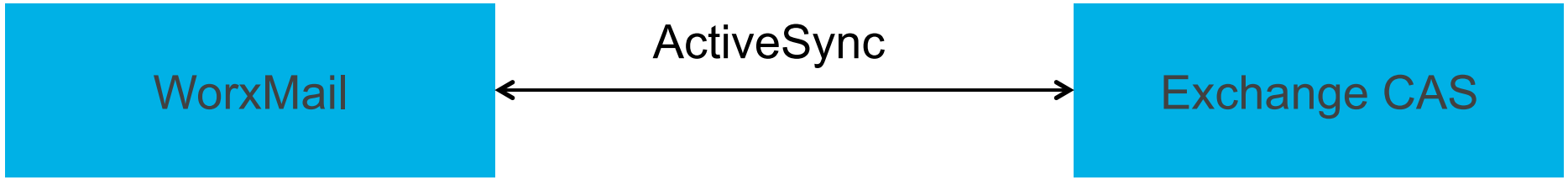
```
add vpn trafficPolicy bypass_intranet "REQ.HTTP.HEADER CSHOST CONTAINS
mycompany.com" allow_intranet

bind vpn vserver MyVPN-policy Allow_intranet
```

WorxWeb with NetScaler Proxy config

	iOS SecureBrowse	iOS MicroVPN	Android SecureBrowse	Android MicroVPN
HTTP	✓	✓	✓	✓
HTTPS	✓	✓	✓	✓
HTTP w/ 401 SSO	✓	✓	✓	✓
HTTPS w/401 SSO	✓	✗	✓	✗
HTTP via Proxy	✓	✓	✓	✓
HTTPS via Proxy	✗	✓	✗	✓
HTTP via proxy w/ 407 SSO	✓	✓	✓	✓
HTTPS via proxy w/ 407 SSO	✗	✗	✗	✗
HTTP via proxy w/ 407 and 401 SSO	✓(NS 10.5)	✓	✓(NS 10.5)	✓
HTTPS via proxy w/ 407 and 401 SSO	✗	✗	✗	✗

*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

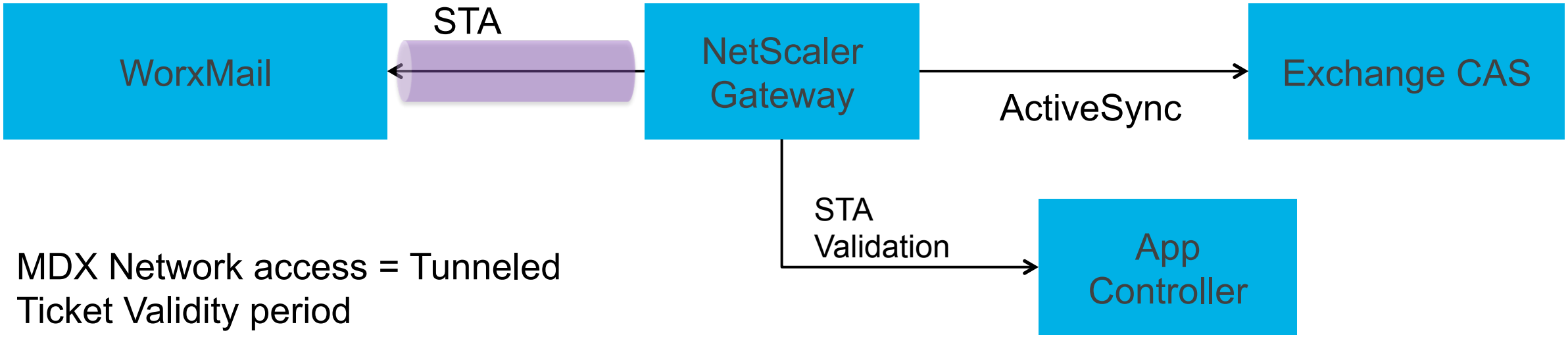
Pros

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

Cons

1. Poor device battery life

RECOMMENDED WORXMAIL DEPLOYMENT

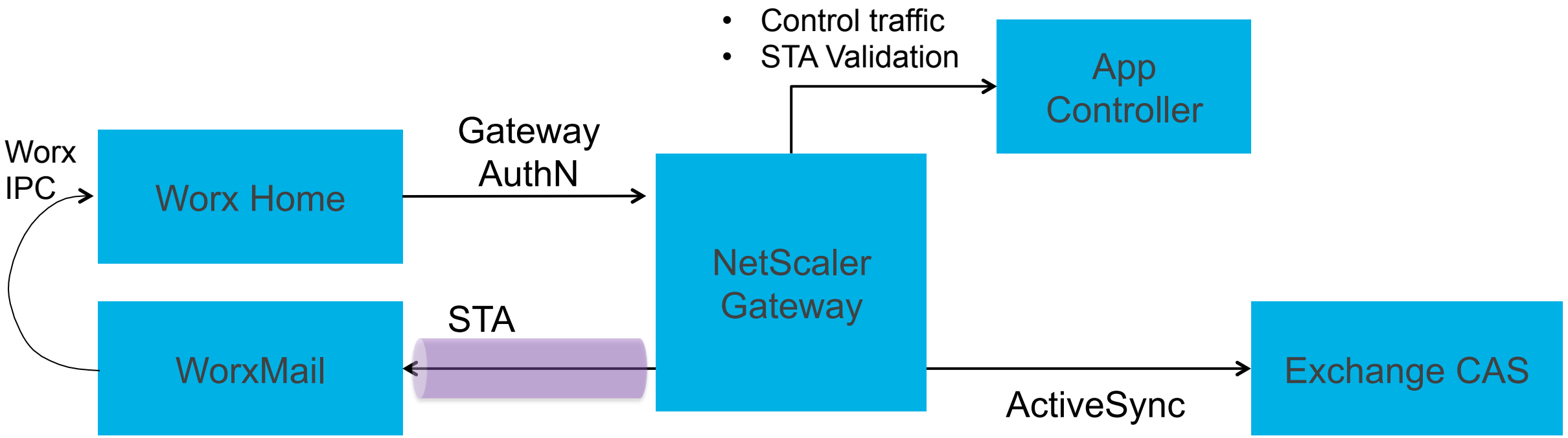


MDX Network access = Tunneled
Ticket Validity period
Background services gateway
STA provider config on NetScaler Gateway

Pros

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

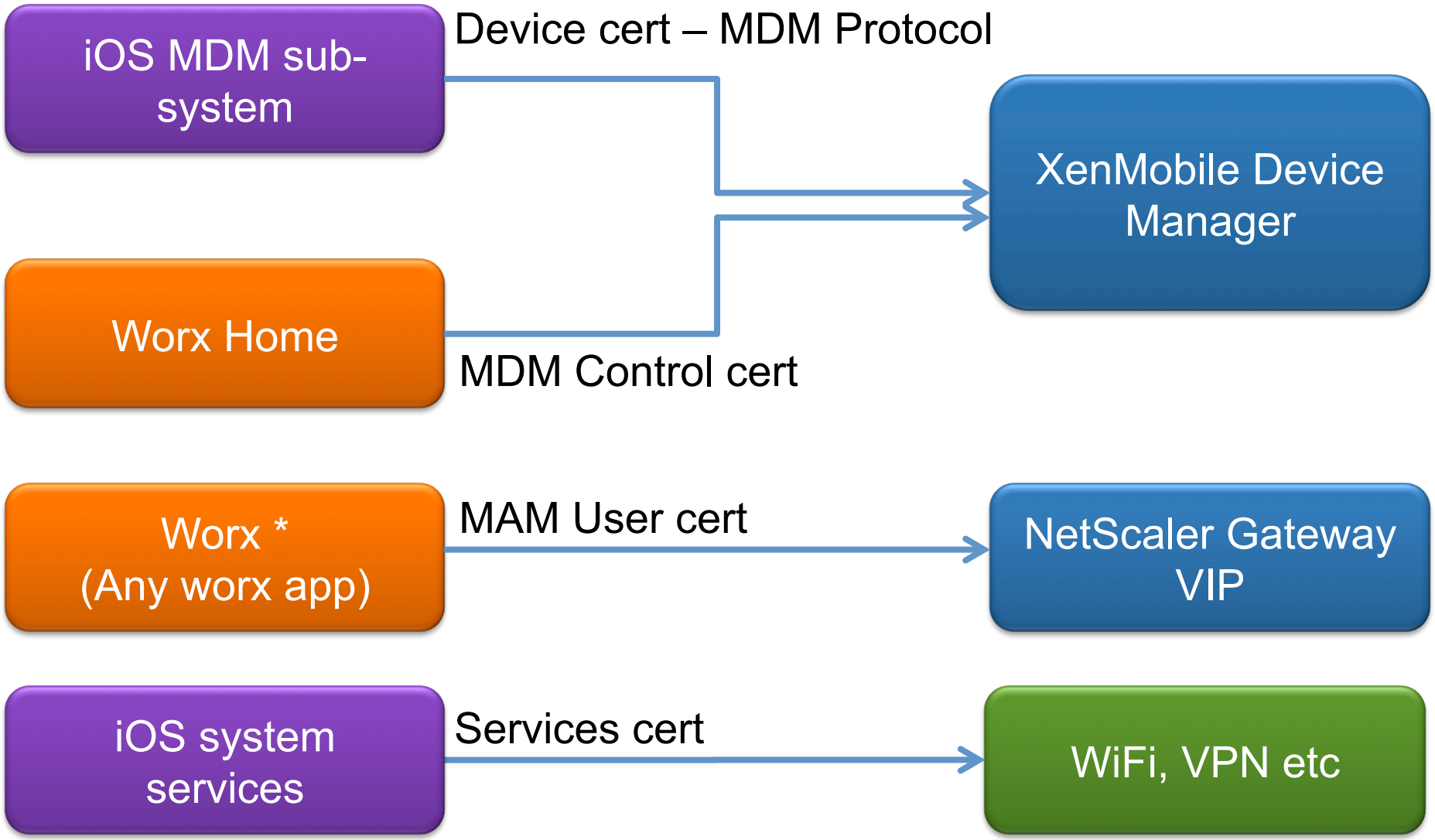
TRAFFIC FLOW



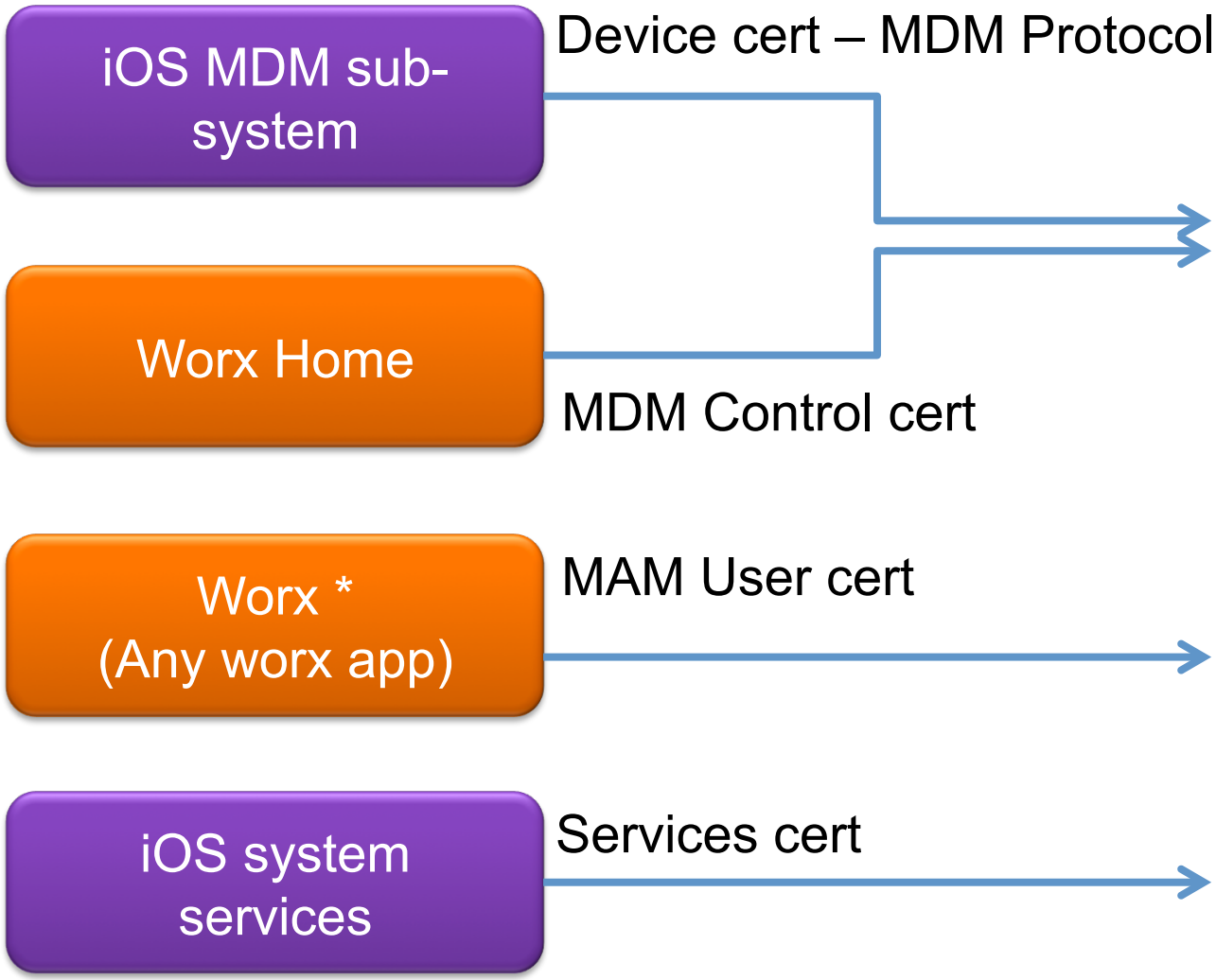
1. Worx Home authN at NetScaler Gateway VIP based on configured authN policy
2. All control communication with App Controller
3. WorxMail token retrieval from Worx Home
4. WorxMail data connection to NetScaler Gateway and onward to CAS

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

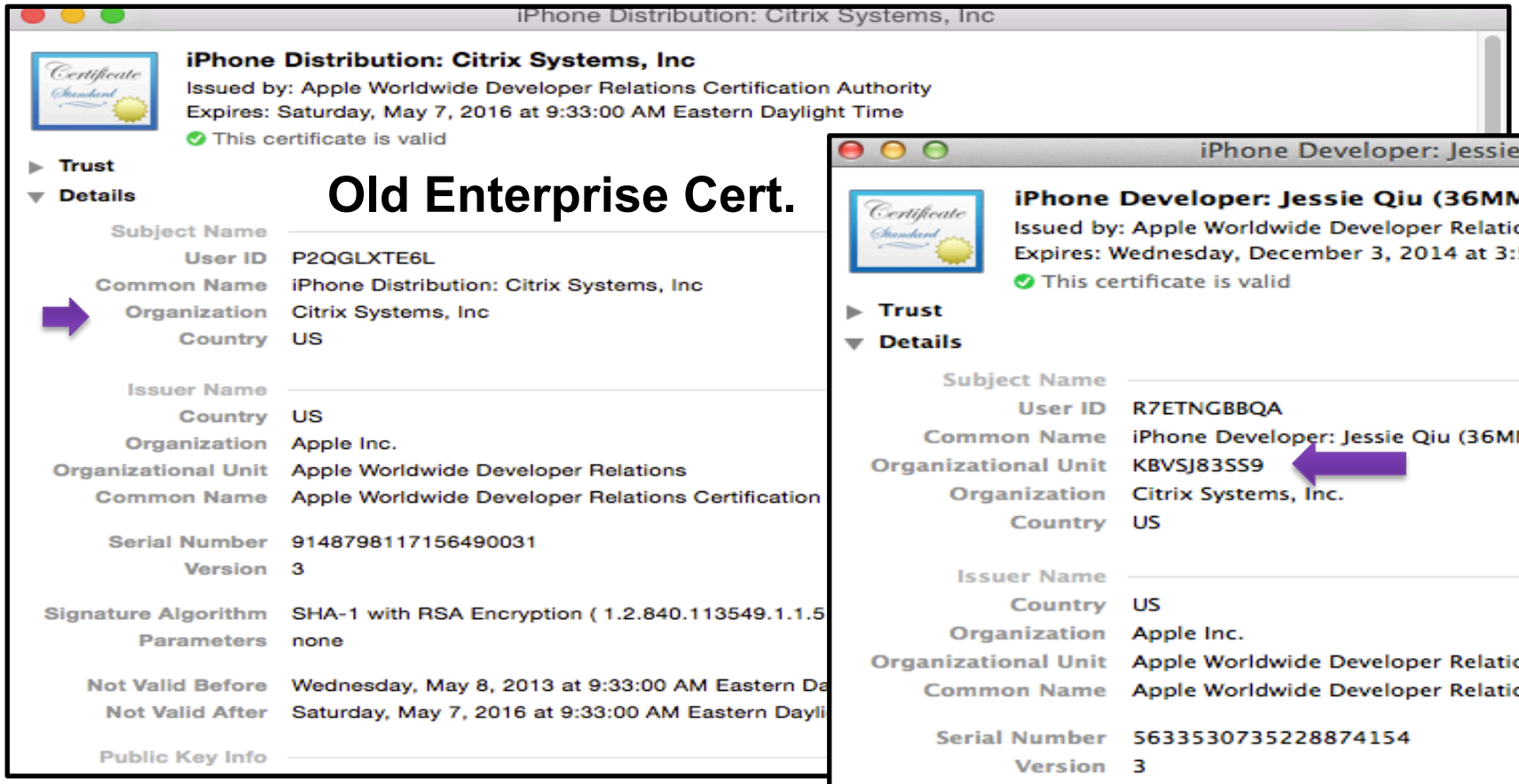
Apps need to be re-wrapped using MDX 9.0.2+

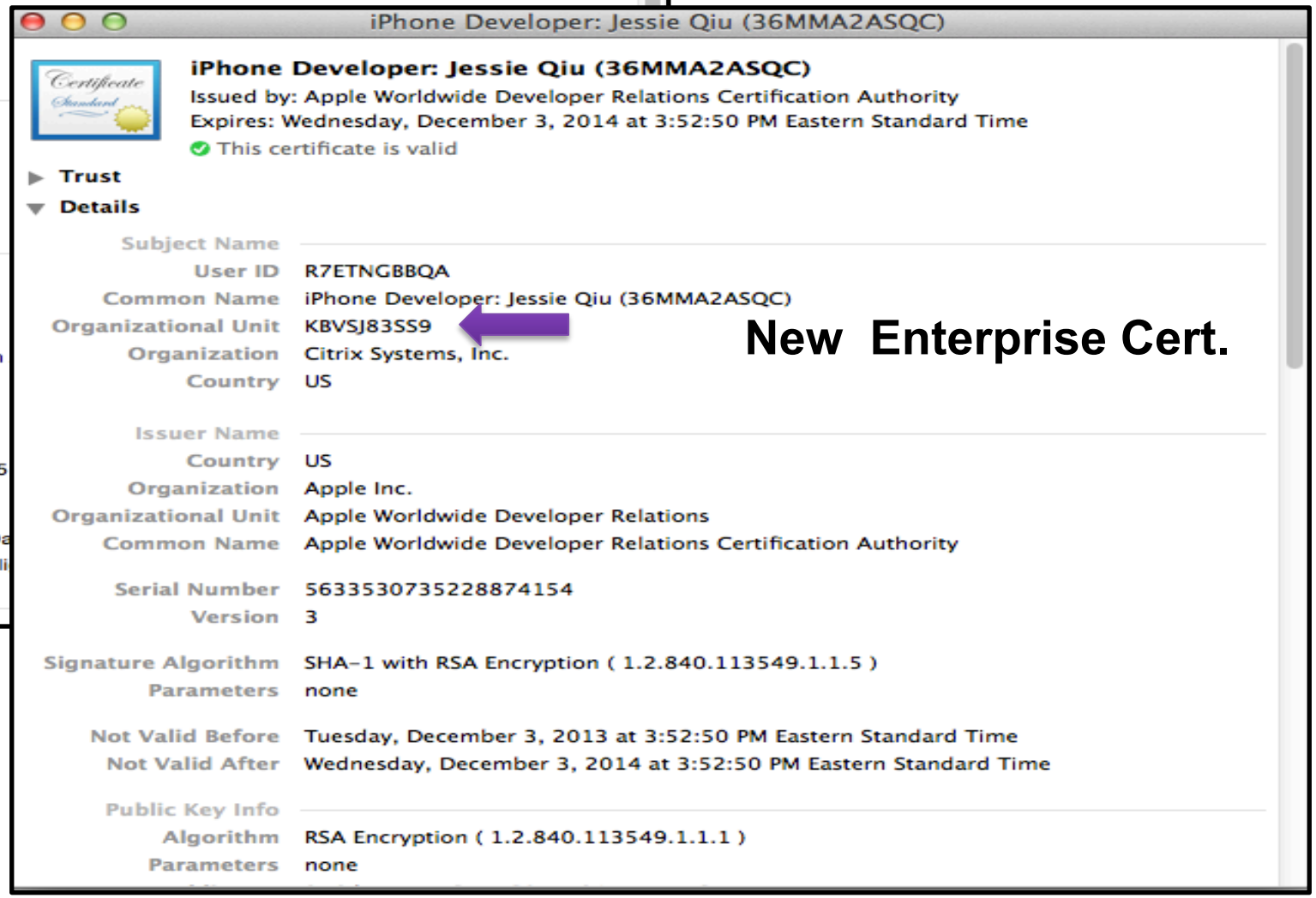
Verify signing cert and provisioning profile for team ID and OU

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>MIIFlTCCBH2gAwIBAgIIKdSidnQKrAswDQYJKoZIhvcNAQEFBQAwgZYxCzAJBgNVBAYTAlVTMRMwEQYDVQQKDApBcHBsZSBJbmMuMSwwKgYDVQQLDCNBcHBsZSBXb3JsZHdpZGUgRGV2ZWxvcGVyIFJlbGF0aW9uczFEMEIGA1U
ww7QXBwbGUgV29ybGR3aWRlIERldmVsb3BlciBSZWxhdGlvbnMgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMTQwODIxMTU0MDUyWhcNMTUwODIxMTU0MDUyWjCBiDEaMBgGCgmSJomT8ixkAQEMCjk5NjhOQUJHQVMxNDAyBgNV
MMK2lQaG9uZSBEaXN0cmlidXRpb246IERhdmlkIEhveSAoOTk2OE5BQkdBUykxEzARBgNVBAsMCjk5NjhOQUJHQVMxEjAQBgNVBAoMCURhdmlkIEhveTELMAkGA1UEBhMCVVMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBA
U3Bkv3MK7bF9WCzQFwEwFVmq7aXBvBCap5wLhCoqRuuTwkOK7CZk0l7U9Og9CTb6tSSTzrM/GRzSB5EJv2SREg6VZw1qGkfmgzPDGmpmxEUMp7sxTf9rbplBfmN6BUYnpN4tu
Meoa95bUJKEM0kZvtQ0DTjMdX2IgUPKpo4I1rxLxqD4WVTlPwHBDvCq94qVYHCcnPNYZEADrvRyBtSlWuU6CqCFgYPCY/
feIIWdbaFhW6ZmHd9xRlpaONCZZ4OHffKeh0P6uz1ebyMAANo1jKRwkNQG0Z5zq0cyvermN0FFIt734UlzJxhhxcTvRdHJSl1y4e4rLoKmeXrPhAgMBAAGjggHxMIIB7TAdBgNVHQ4EFgQUCXybmq2EbTJpD4VXZ1czTnecCS4wDAYD
0TAQH/BAIwADAfBgNVHSMEGDAWgBSIJxcJqbYYYIvs67r2R1nFUlSjtzCCAQ8GA1UdIASCAQYwggECMIH/
kqhkiG92NkBQEwgfEwgcMGCCsGAQUFBwICMIG2DIGzUmVsaWFuY2Ugb24gdGhpcyBjZXJ0aWZpY2F0ZSBieSBhbnkgcGFydHkgYXNzdW1lcyBhY2NlcHRhbmNlIG9mIHRoZSB0aGVuIGFwcGxpY2FibGUgc3RhbmRhcmQgdGVybXMgY
kIGNvbmRpdGlvbnMgb2YgdXNlLCBjZXJ0aWZpY2F0ZSBwb2xpY3kgYW5kIGNlcnRpZmljYXRpb24gcHJhY3RpY2UgcHVibGlzaGVkIGF0IGh0dHA6Ly93d3cuYXBwbGUuY29tL2FwcGxlY2EvME0GA1UdHwRGME
QqBAoD6GPGh0dHA6Ly9kZXZlbG9wZXIuYXBwbGUuY29tL2NlcnRpZmljYXRpb25hdXRob3JpdHkvd3dkcmNhLmNybDAOBgNVHQ8BAf8EBAMCB4AwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwMwEwYKKoZIhvdjZAYBBAEB/
CBQAwDQYJKoZIhvcNAQEFBQADggEBAG8xiUxK+fUjIRlosnc7sB1DUCo21Ki7C4ai
tDtP7Y1dtryPROscbQoeO8wddauakVMQxUFAn8tT9J0+4juSQlq4nQmuftIgH950nVN3BX8yC0ZbMUw37W5kiU9oII79b6AYXDN5DW0kx7Xj7aQQ+AqaSqLESC7t61lzH+bLCdudHNtEgzht8xnL98MiUci1PVVXN3EO/
LQE9DxNiS8ZrkhY0z/hmN1YCQgHJFso51bycZPJNvBqC+NaOrGMm/26F5zMeZY1PvE+g5/SUyrL8yO7T3XuUJdMUy+zFks+62yqPYoreXHMFJQ6fM9ICoYAXv5HMx9X3emrZUrzq4g=</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>
```





Log file

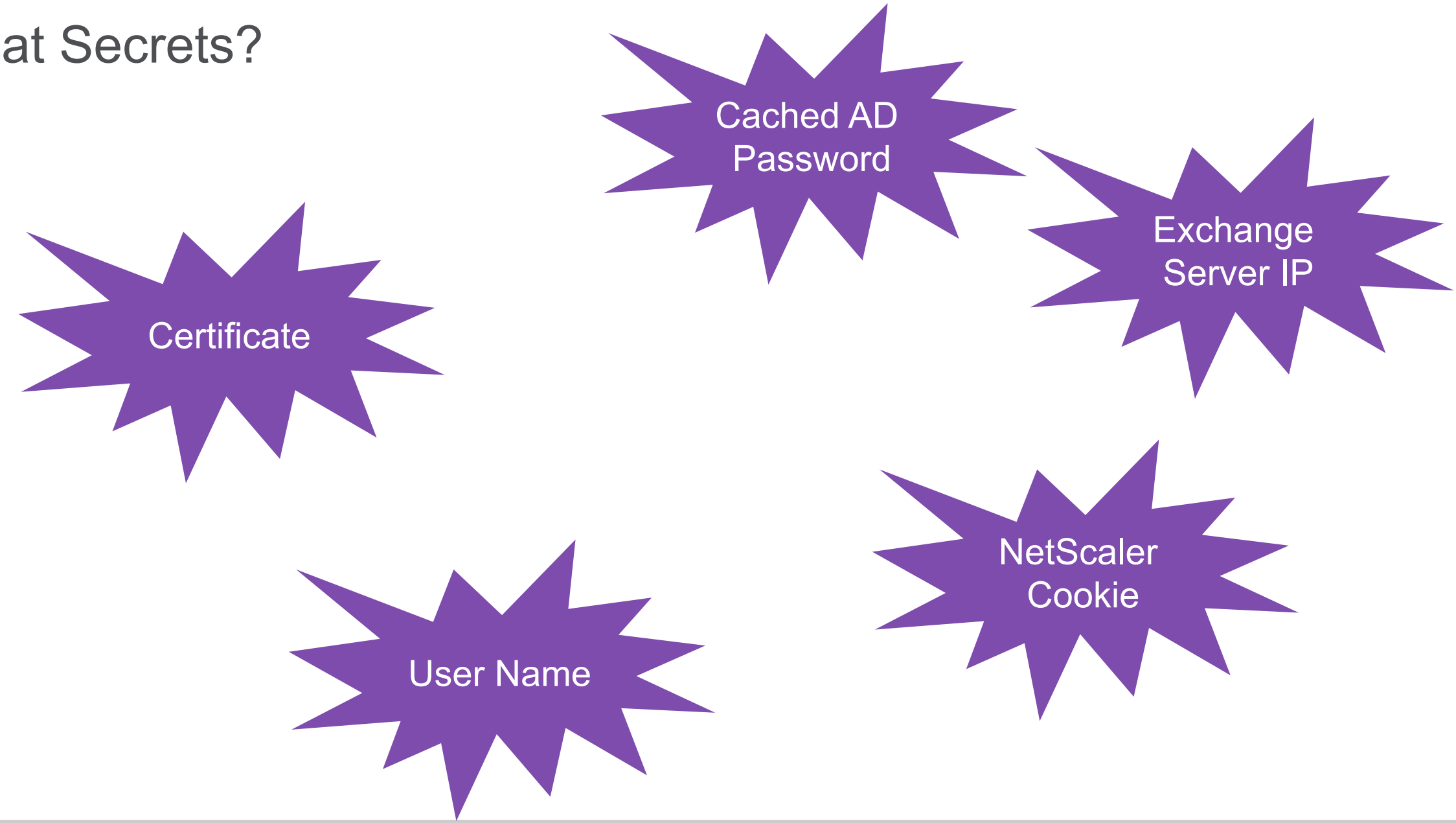
MySample(pid 964) - [deny-mmap] mapped file has no team identifier and is not a platform binary:

Secrets Vault

User Entropy, System Entropy etc

36

What Secrets?



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:

- 1st hurdle – Jailbreak device and access KeyChain
- 2nd hurdle – Identify the right element in keychain for attack
- 3rd hurdle – Secrets Vault appears to be a meaningless blob
- 4th 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

QUALYS® SSL LABS

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

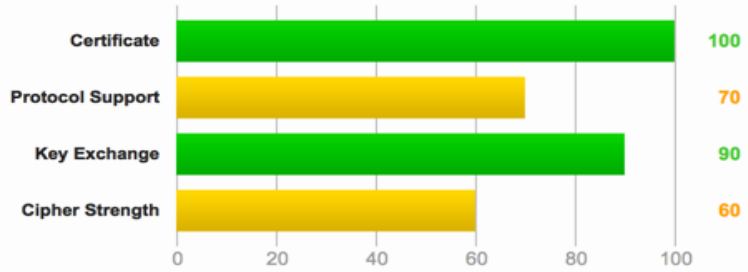
Assessed on: Fri Oct 17 02:31:51 PDT 2014 | Clear cache

Scan Another »

Summary

Overall Rating

B



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

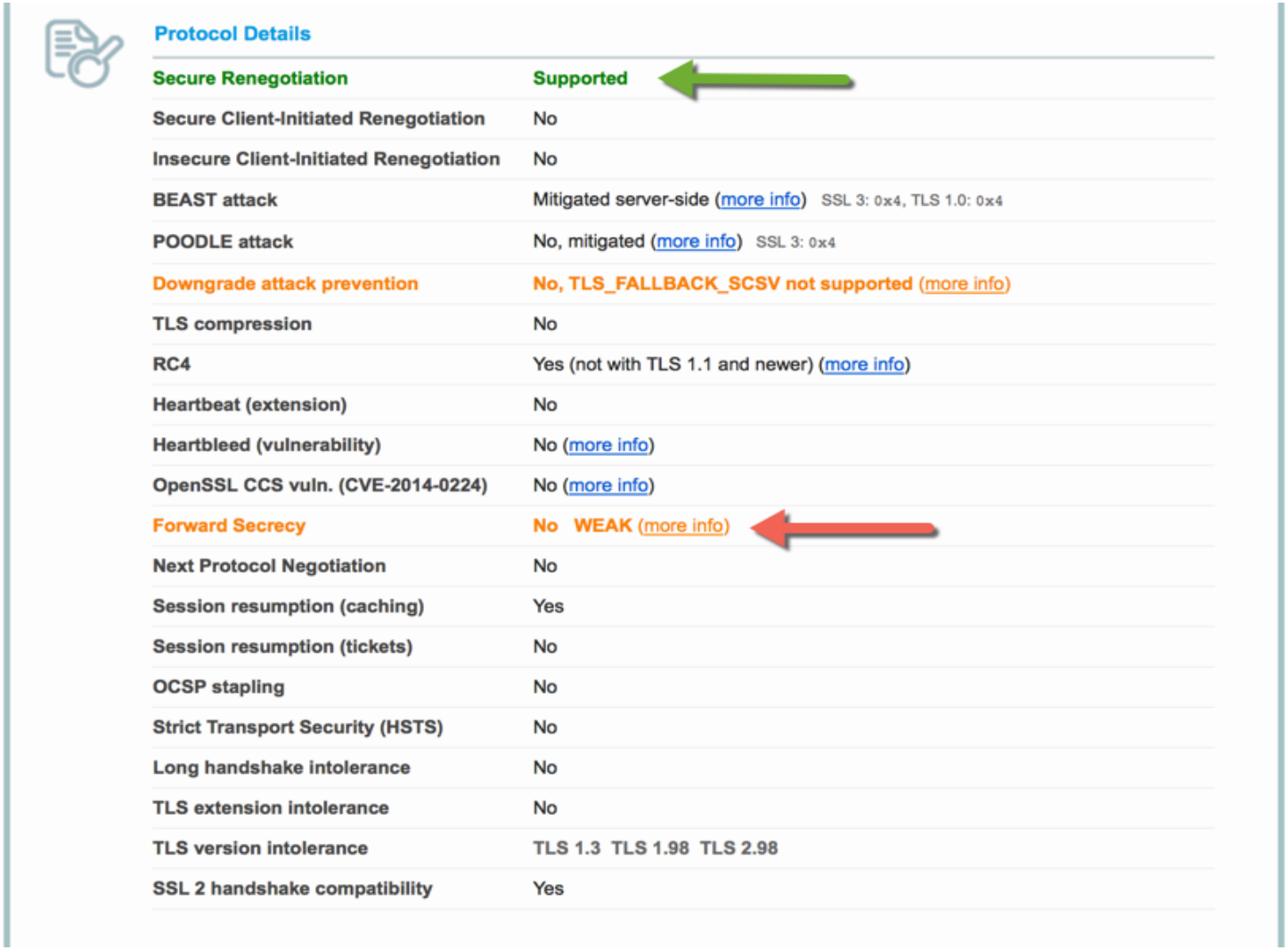
Protocols

TLS 1.2	No
TLS 1.1	No
TLS 1.0	Yes
SSL 3 **INSECURE**	Yes
SSL 2	No

Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites always at the end)

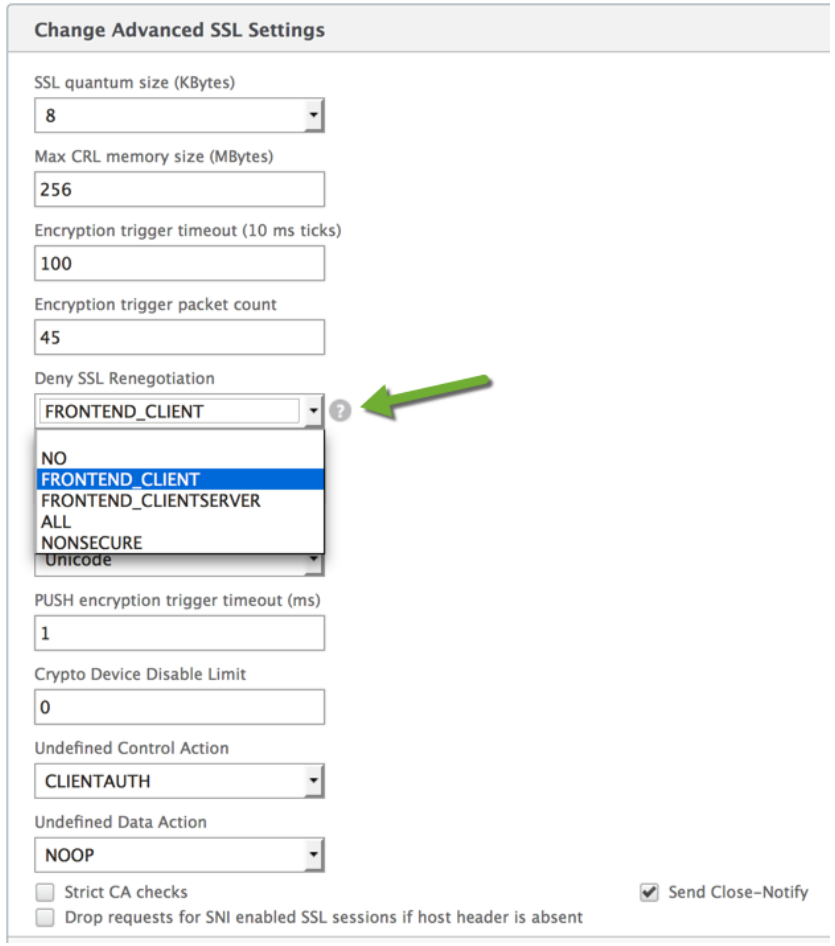
TLS_RSA_WITH_RC4_128_MD5 (0x4)	128
TLS_RSA_WITH_RC4_128_SHA (0x5)	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112
TLS_RSA_WITH_DES_CBC_SHA (0x9) **WEAK**	56
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_DES_CBC_SHA (0x9) **WEAK**	56

No Perfect Forward Secrecy but finally no Renegotiation



Protocol Details

Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info) SSL 3: 0x4, TLS 1.0: 0x4
POODLE attack	No, mitigated (more info) SSL 3: 0x4
Downgrade attack prevention	No, TLS_FALLBACK_SCSV not supported (more info)
TLS compression	No
RC4	Yes (not with TLS 1.1 and newer) (more info)
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy	No WEAK (more info)
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



Generating DH Key for FS

NetScaler VPX (3000)

Info
NS10.5 51.1017.e.nc

Dashboard | Configuration | Reporting | Documentation

- + System
- + AppExpert
- − Traffic Management
  - + Load Balancing
  - + Content Switching
  - + Cache Redirection
  - + DNS
  - + GSLB
  - + SSL
- + Optimization
- + Security
- + NetScaler Gateway

Show Unlicensed Features

Integrate with Citrix Products

XenMobile

NetScaler > Traffic Management > SSL

Getting Started
Server Certificate Wizard
Client Certificate Wizard
Intermediate-CA Certificate Wizard
Root-CA Certificate Wizard
CRL Management

SSL Certificates
Create CSR (Certificate Signing Request)
Create Certificate
Create and Install a Server Test Certificate

SSL Keys
Create RSA Key
Create DSA Key

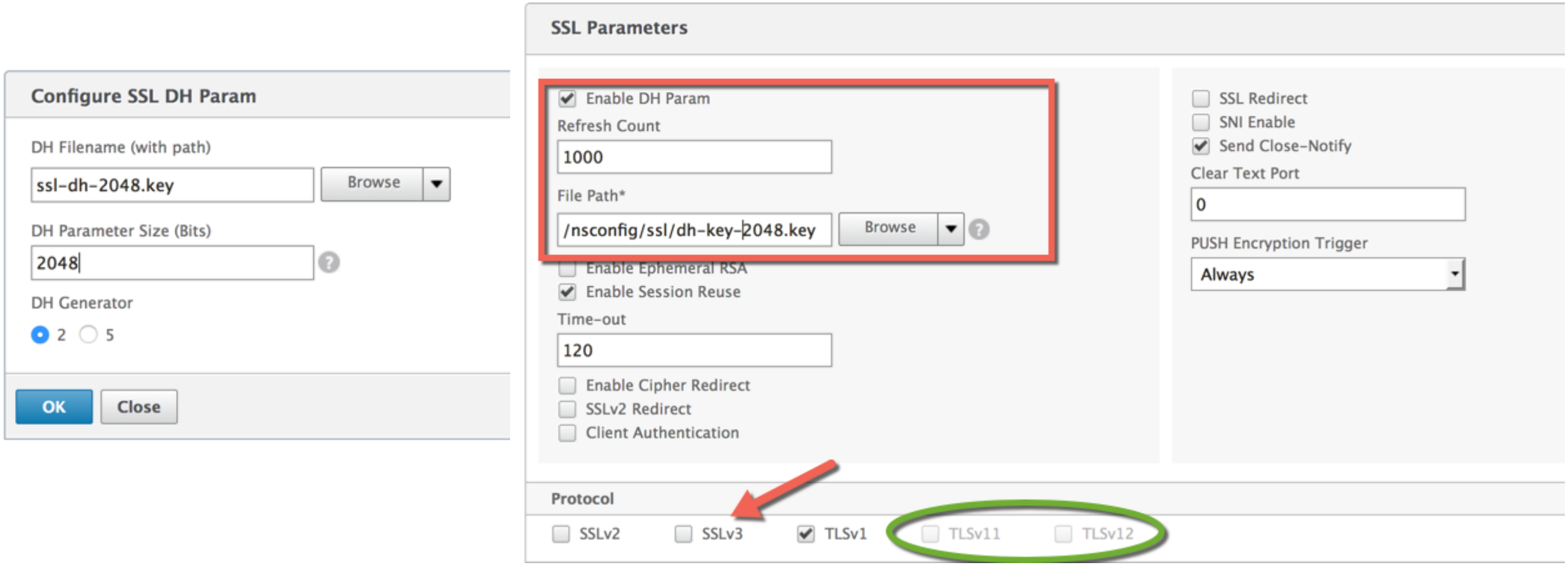
Tools
Create Diffie-Hellman (DH) key
Import PKCS#12
Export PKCS#12
Manage Certificates / Keys / CSRs
Start SSL certificate, key file synchronization for HA
Start SSL certificate, key file synchronization for Cluster
OpenSSL interface

Policy Manager
SSL Policy Manager

Settings
Change advanced SSL settings

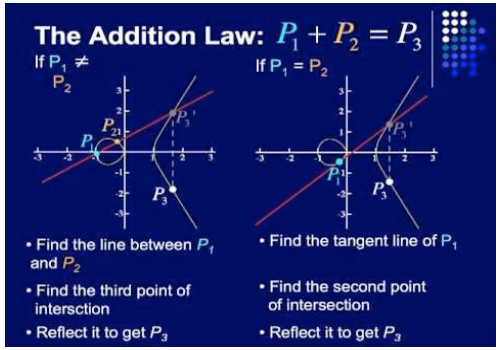
Configuration Summary
5 Certificate-key pairs

Vserver SSL settings



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> -ciperName YOUR-DEFAULT-ECCPFS

Bind ECC curves to SSL Vserver

- bind ssl vserver <vserverName> -eccCurveName ALL

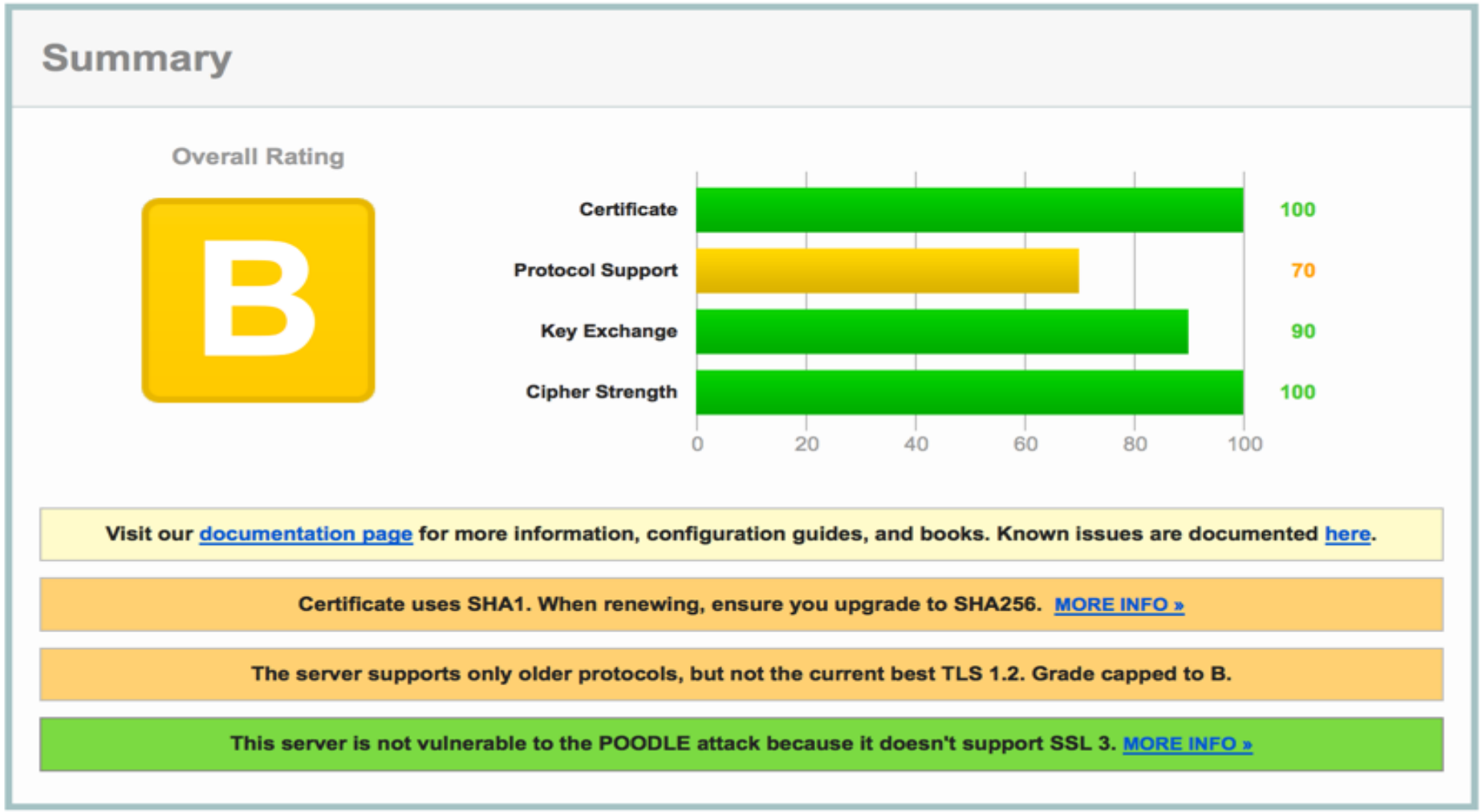
  (Only on VPX and MPX/SDX115xx and higher)

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+)

QUALYS® SSL LABS



Just the Ciphers we want

Configuration

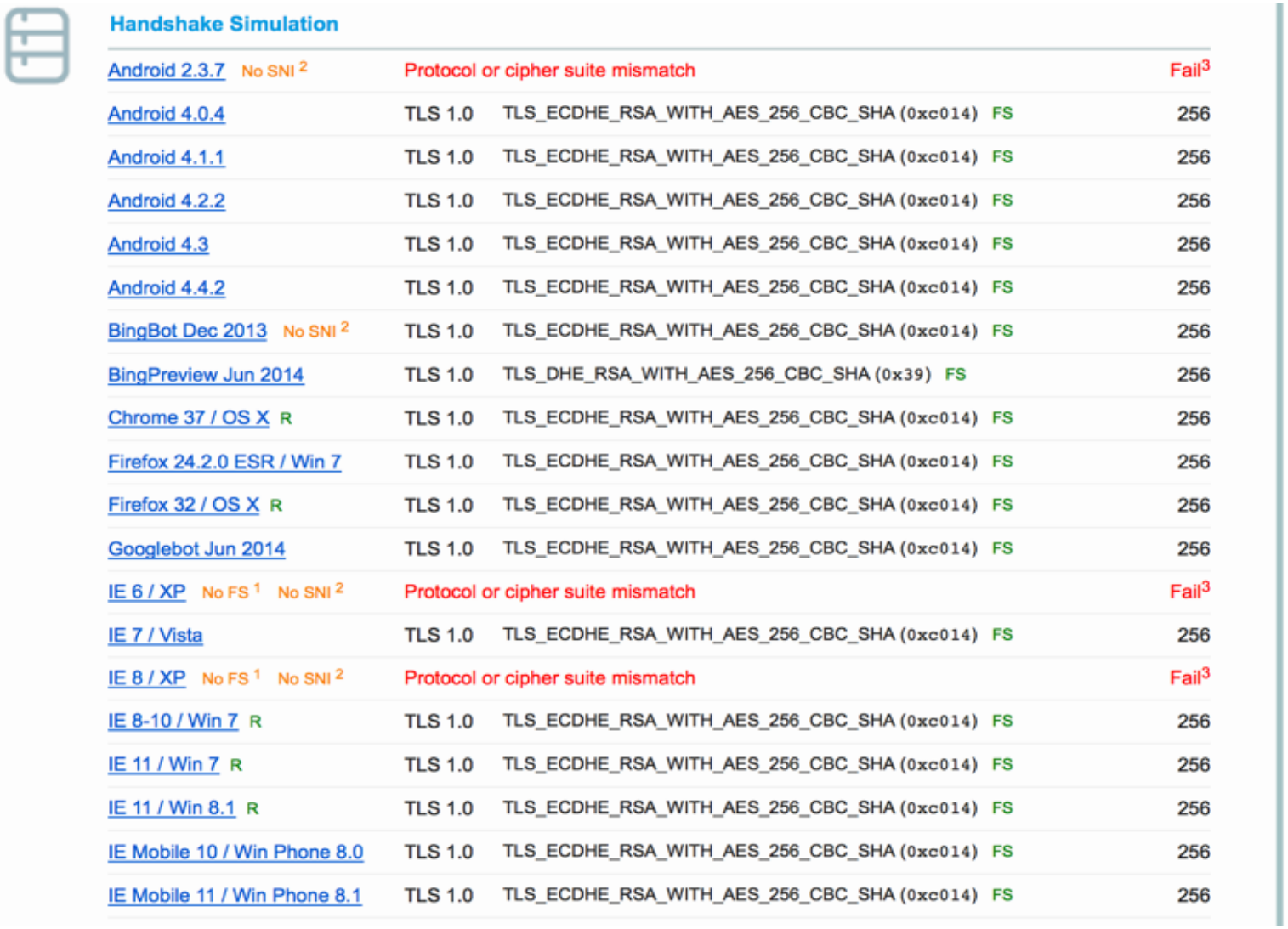
Protocols

TLS 1.2	No
TLS 1.1	No
TLS 1.0	Yes
SSL 3	No
SSL 2	No

Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites always at the end)

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH 256 bits (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits (p: 256, g: 1, Ys: 256) FS	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		256

Forward Secrecy on all supported platforms



Handshake Simulation

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

Network Tracing

Technical Preparation:

Certificates: **Xen**Mobile Server-side

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

- **Xen**Mobile **MDM:** cert *tied to the MDM FQDN* – secures the trusted MDM enrollment of devices and allows for SSO capabilities later.
- **Xen**Mobile **MAM:** cert *tied to the **Net**Scaler Gateway FQDN* for the **Xen**Mobile 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

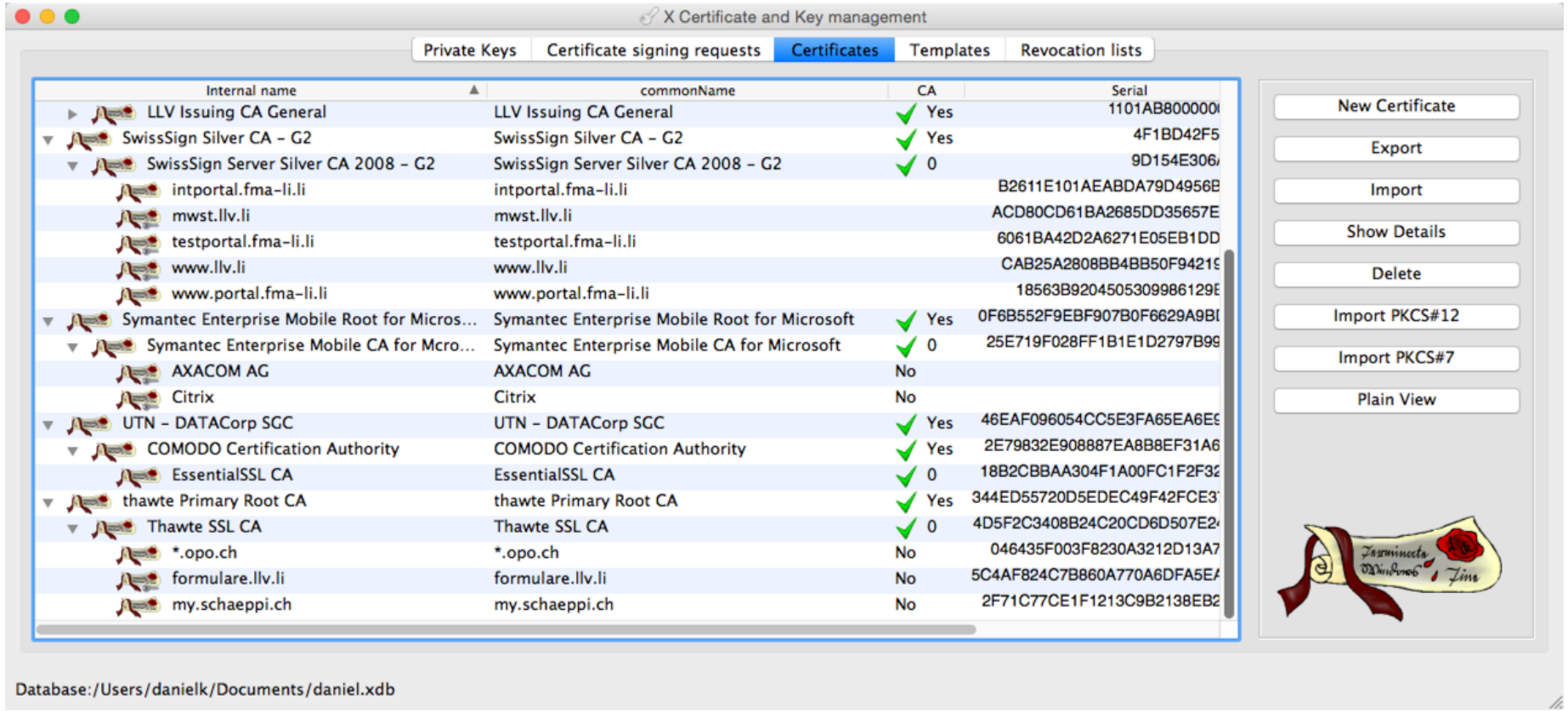
OpenSSL

```
# 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

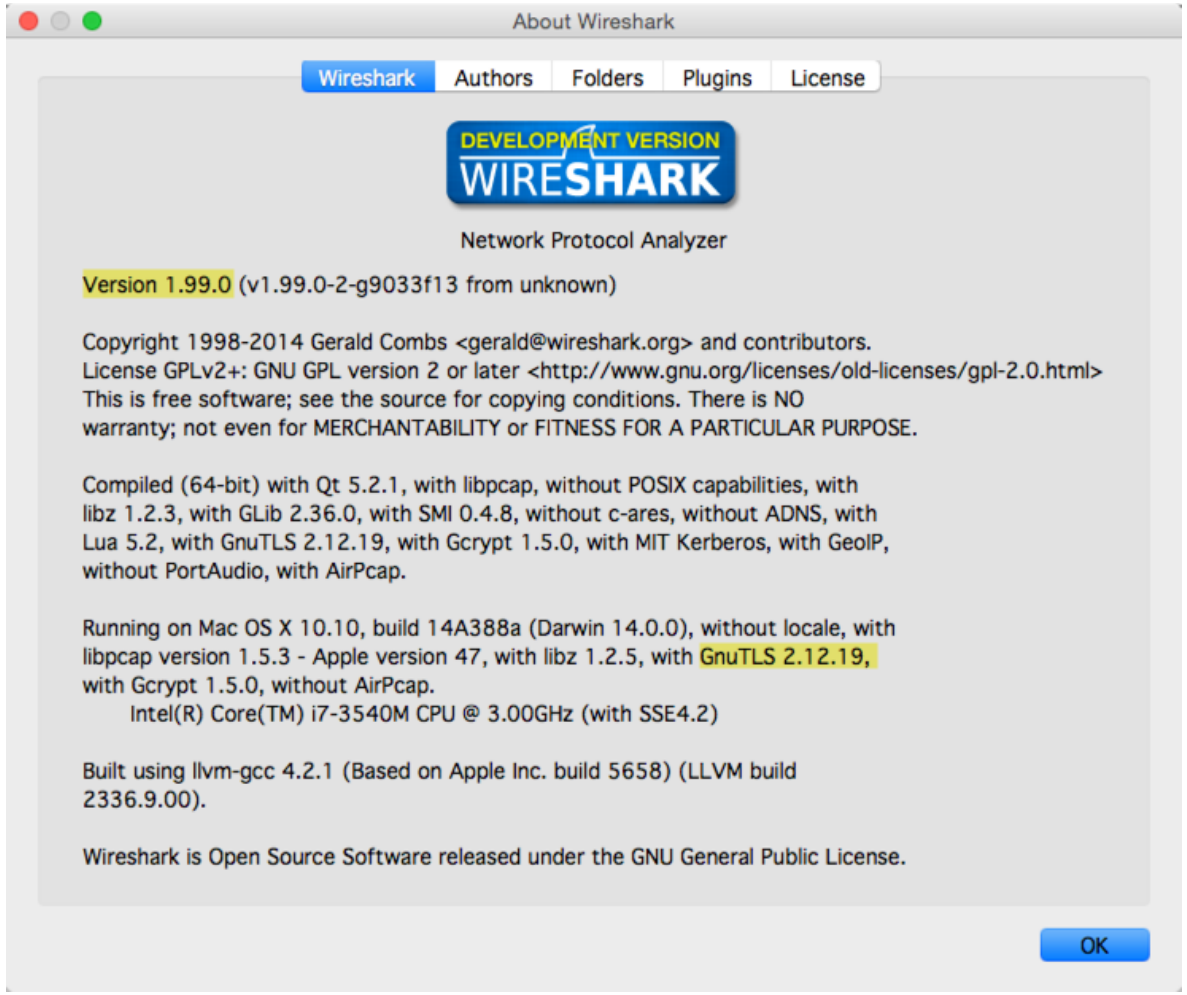


Troubleshooting

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

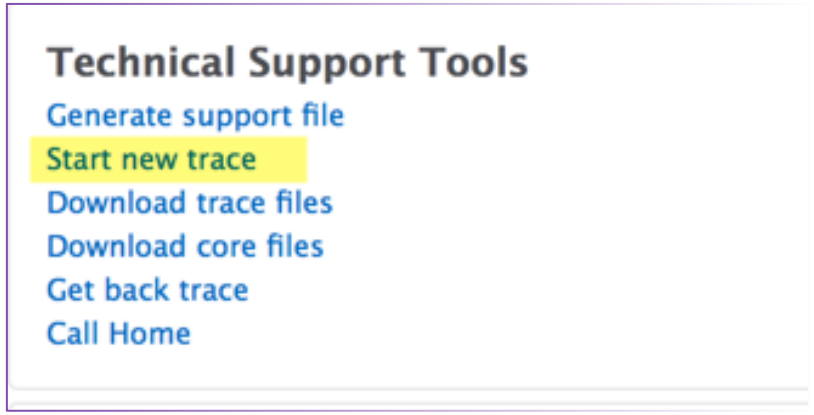


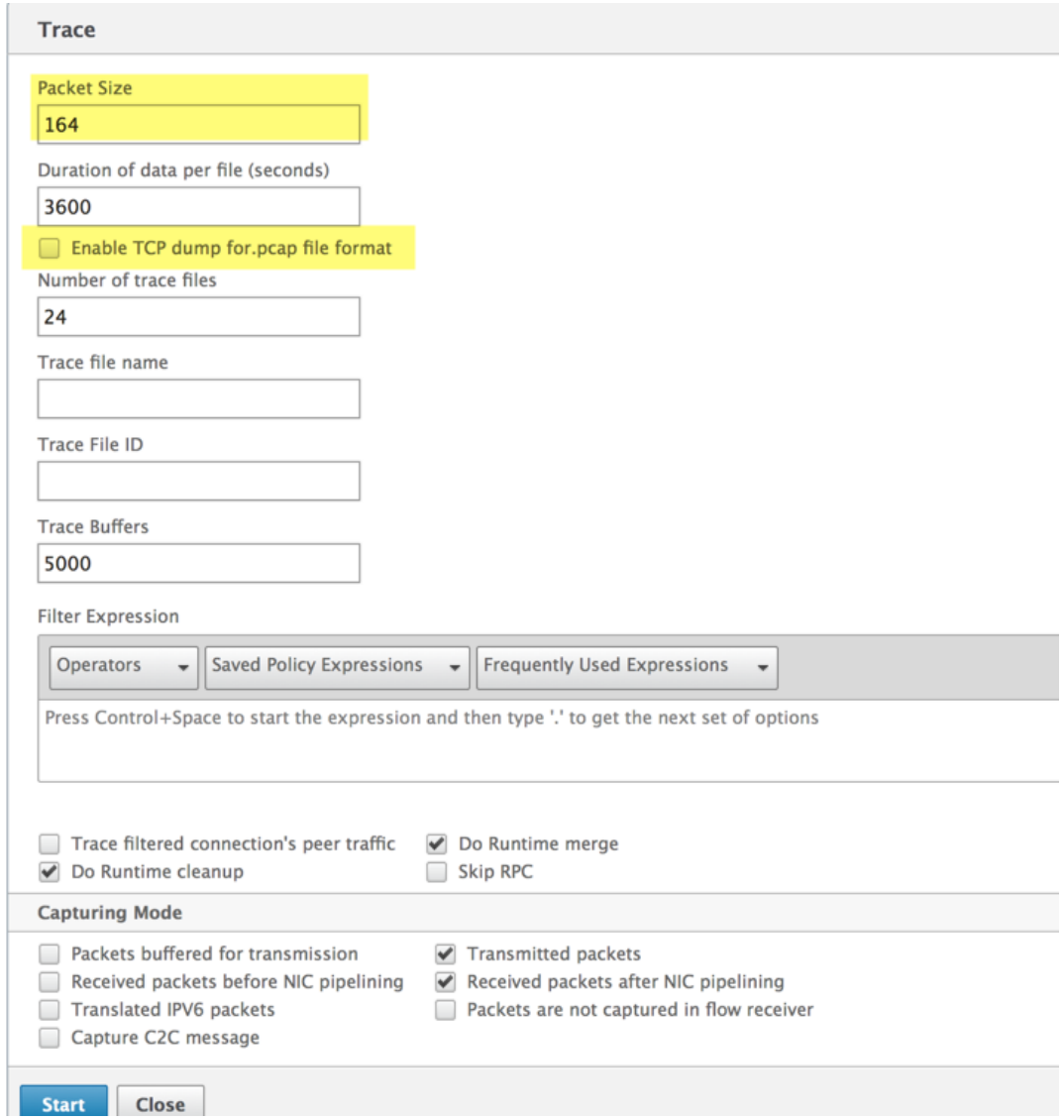
Troubleshooting

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)

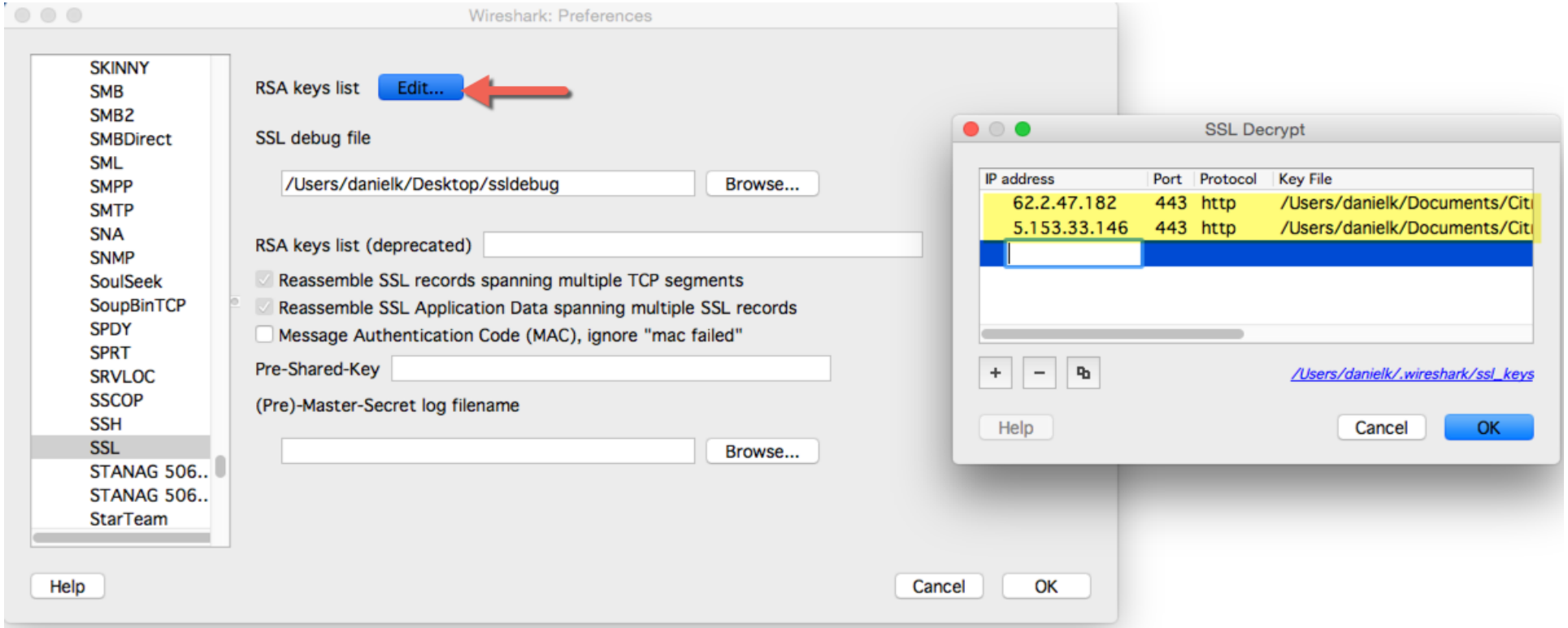




Troubleshooting

Using Wireshark

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

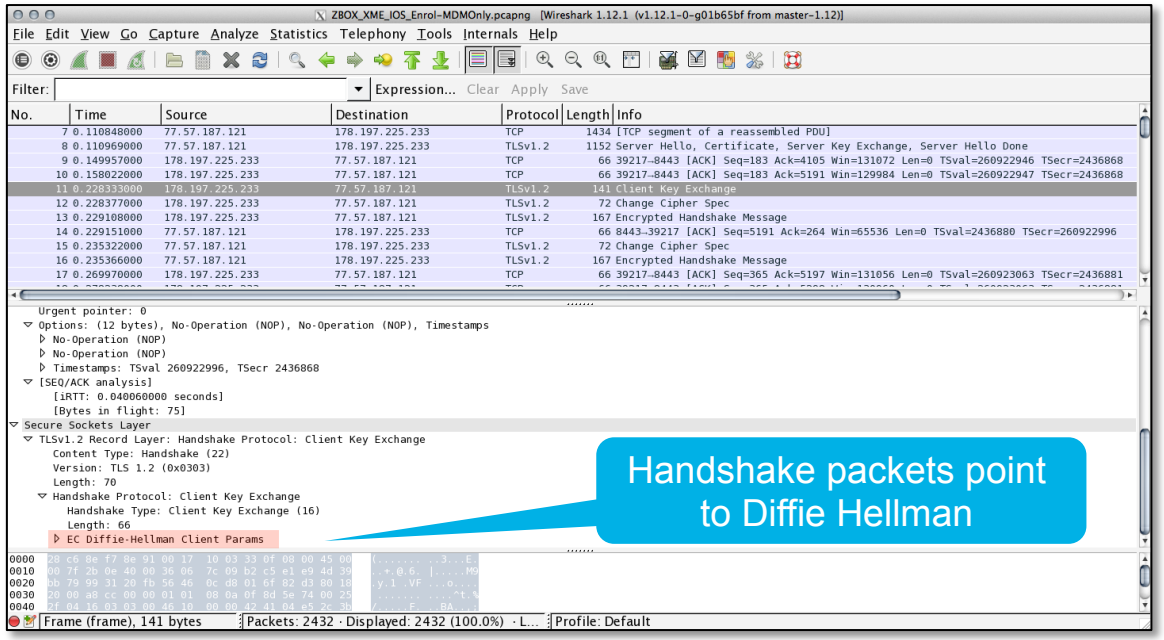


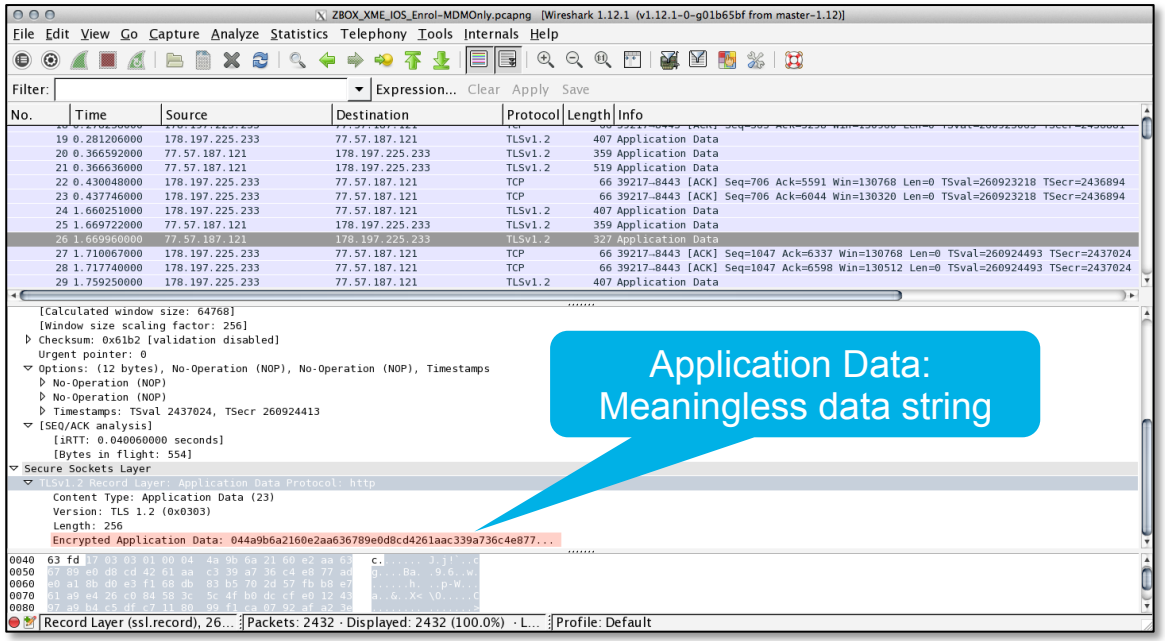
Troubleshooting

Using Wireshark

DH Keys can’t be used to decipher SSL traffic

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

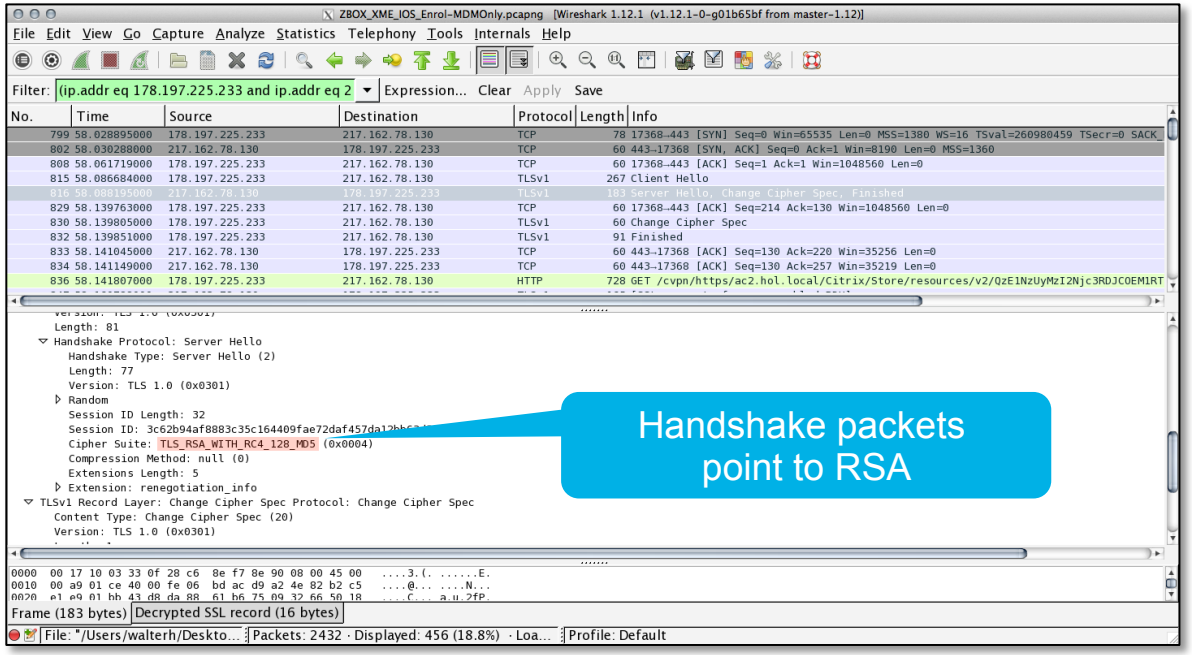


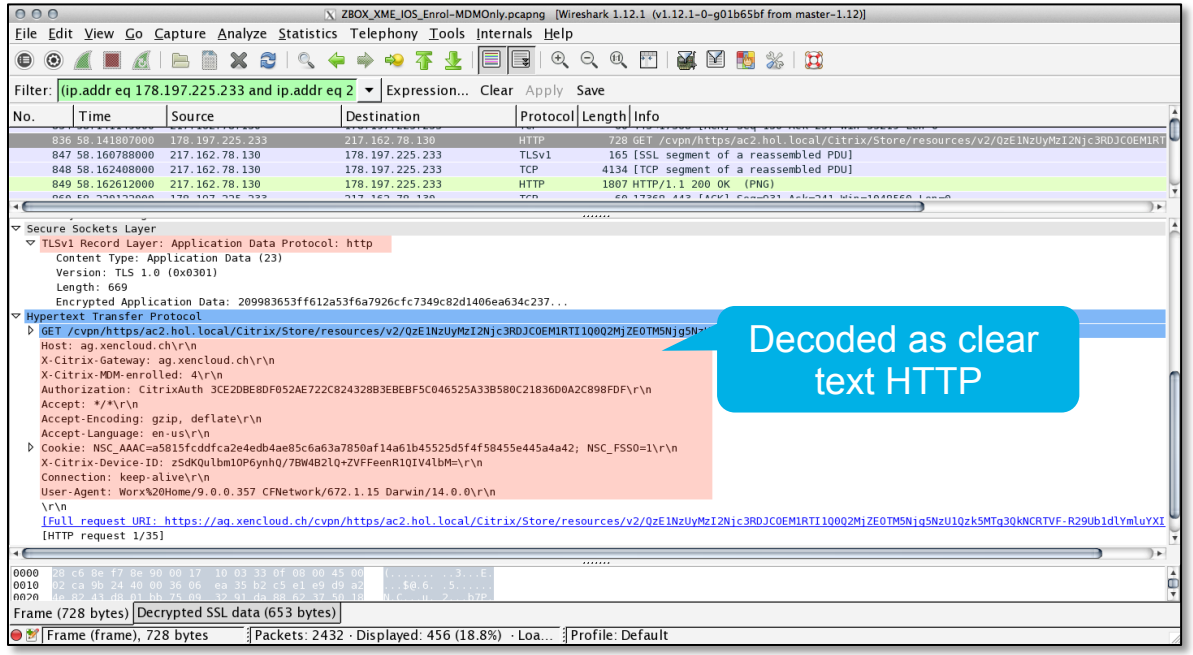


Troubleshooting

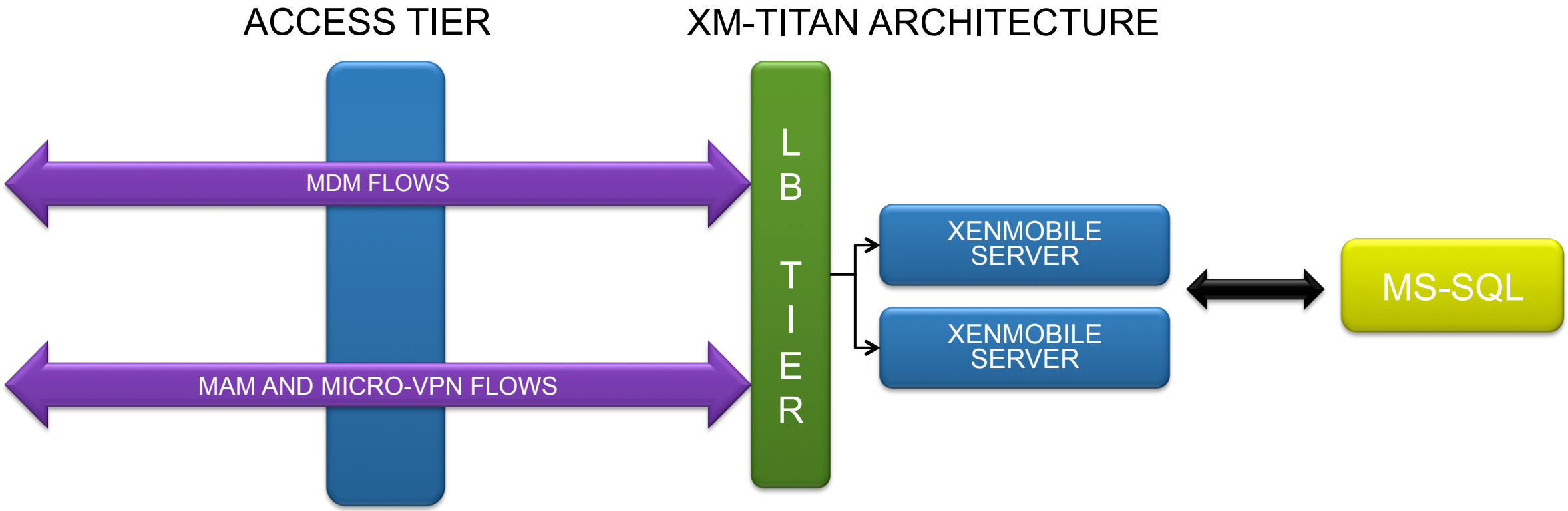
Using Wireshark

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





Titan - Preview



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

MDM Endpoint Interface

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

DB

- MS SQL 2012+
- DR with DB replication

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

MAM Endpoint Interface

- Listening on ports 443 (non-cert based)

PKI

- No change from XM9
  - MSFT CA for user certs

Unified console

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

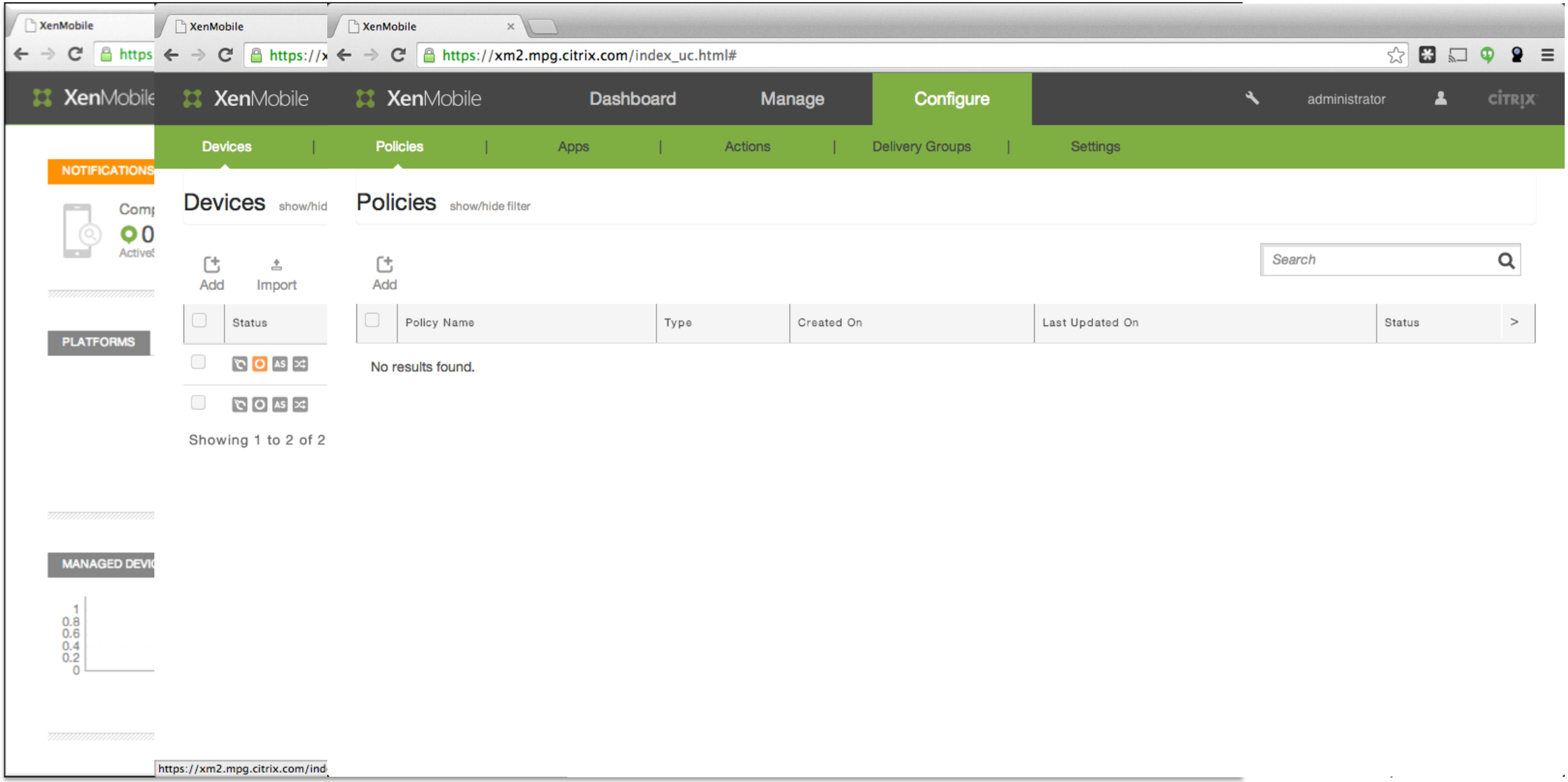
API

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

Syslog

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

Unified Administrative Console




Ein Unternehmen der ADN® Gruppe
BCD SINTRAG
value add distribution


CITRIX®