Ondřej Ševeček | GOPAS a.s. |
MCM: Directory Services | MVP: Enterprise Security |
ondrej@sevecek.com | www.sevecek.com |

PUBLISHING RULES

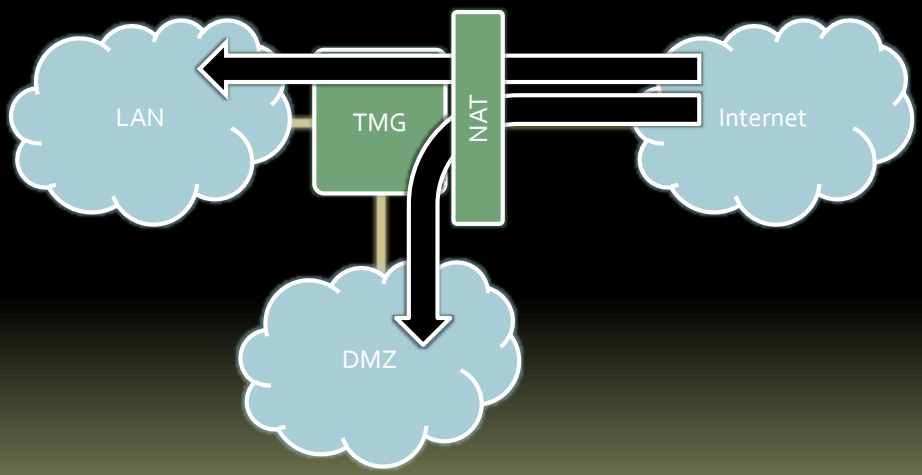
Threat Management Gateway 2010

SERVER PUBLISHING RULES

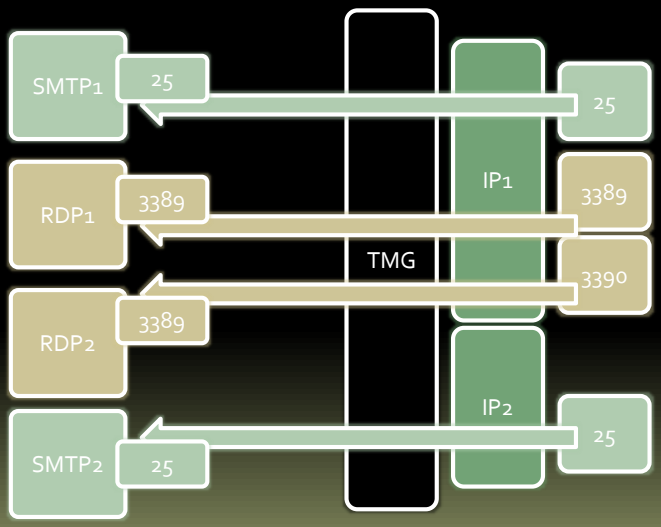
Server Publishing Rules

- Reverse NAT
  - Port Address Translation (PAT)
  - Port Forwarding
- Single public IP : Single port
- Requires NAT network element relationship
  - does not work over route relationship

Publishing (Port Forwarding)



Port Forwarding



Server Publishing

Service	Public IP	Public port	Internal IP	Internal port
SMTP	81.0.0.178	25	10.30.0.31	25
Authenticated SMTP	81.0.0.178	587	10.10.0.16	587
POP3	81.0.0.178	110	10.10.0.16	110
IMAP	81.0.0.178	143	10.10.0.16	143
FTP	81.0.0.178	21	10.30.0.21	21

Lab

- Publish appropriate SMTP, POP3 and IMAP servers
- Publish the FTP server
- Enable FTP upload on the server publishing rule
- From Seven1 placed in Internet, navigate to
  - ftp://gopas-ftp|gopas\kamil:Pa$$word@ftp.gopas.cz
- Upload some content into the FTP server

Threat Management Gateway 2010

EXCHANGE SERVER SMTP NOTES

Send Connectors

- Used for sending outbound email to internet
- Create a new one manually
- Forward either directly (DNS) or through smart-host (may be EDGE)
- Set-SendConnector -Fqdn gopas.cz

Receive Connectors

- Several different connectors
- Must have unique combination of IP/Port/Source IPs
- Change the Default to accept only from internal subnets (used to receive from other Exchange servers)
  - listens on port TCP 25
  - does not allow anonymous access at all
- Leave the Client as it is
  - listens on port TCP 587
  - allows only authenticated client sessions
  - requirest TLS to be started to authenticate

Internet Receive Connector

- New-ReceiveConnector

  -Name InternetAnonymous
  -Fqdn mail.gopas.cz
  -PermissionGroups AnonymousUsers
  -AuthMechanism BasicAuth, Tls, BasicAuthRequireTls
  -Bindings 0.0.0.0:25
  -RemoteIPRanges
  0.0.0.0-10.9.255.255,10.11.0.0-255.255.255.255

- Install a SSL/TLS certificate with the connector's name
  - Enable-ExchangeCertificate -Services SMTP

Antispam Notes

- Sending public IP should
  - be from your own registered IP range or use ISP's smart-host
  - have reverse DNS record pointing into your public domain which is specified on the Send Connector
  - be registered in SenderID public TXT record
- google: SenderID wizard
- www.mxtoolbox.com

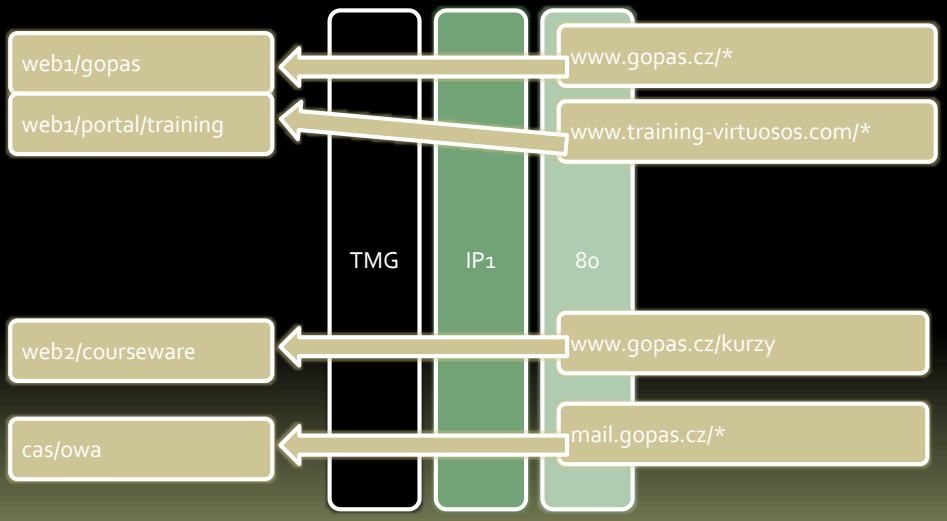
Threat Management Gateway 2010

WEB SERVER PUBLISHING

Web Server Publishing

- Reverse HTTP Proxy
  - Web Listener – listening on public port 80
  - Terminates internet client HTTP connection
  - Forwards as a new request into internal network
- Can publish more web sites on a single IP:port
  - Host header
- Requires NAT network element relationship
  - does not work over route relationship

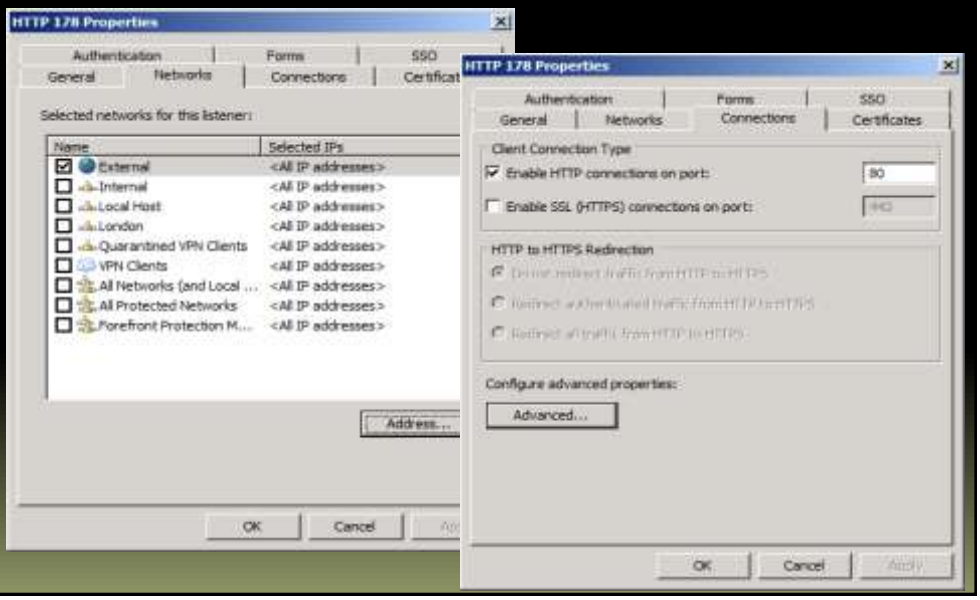
Web Server Publishing



Web Listener

- Proxy server
  - transparent, using port 80
- Must listen on at least one IP address
  - on the public side of the NAT relationship
- Web Listener defines the parameters on the public side from the client
- Web Server Publishing rules define the backend parameters "to" the published server

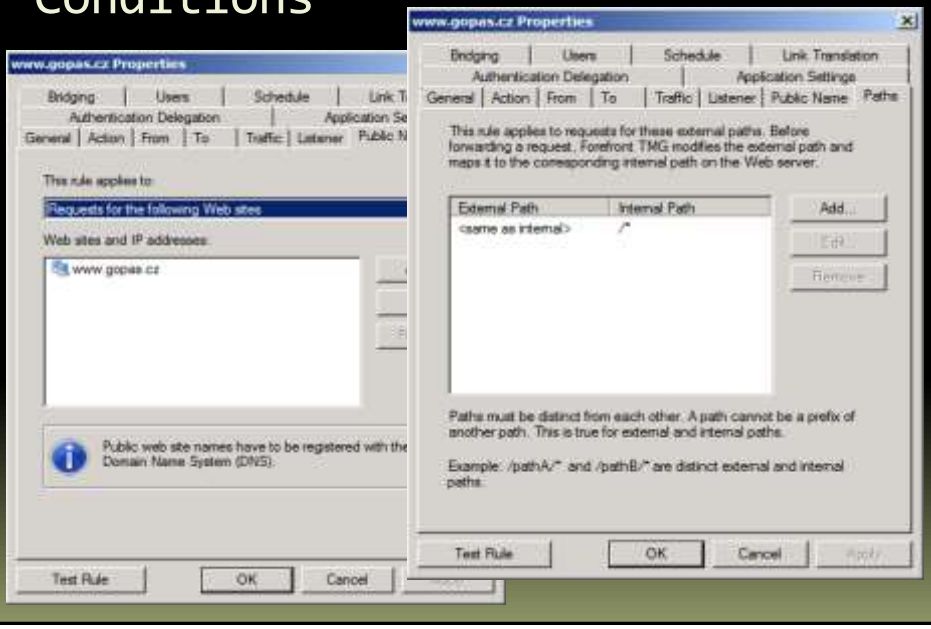
Web Listener



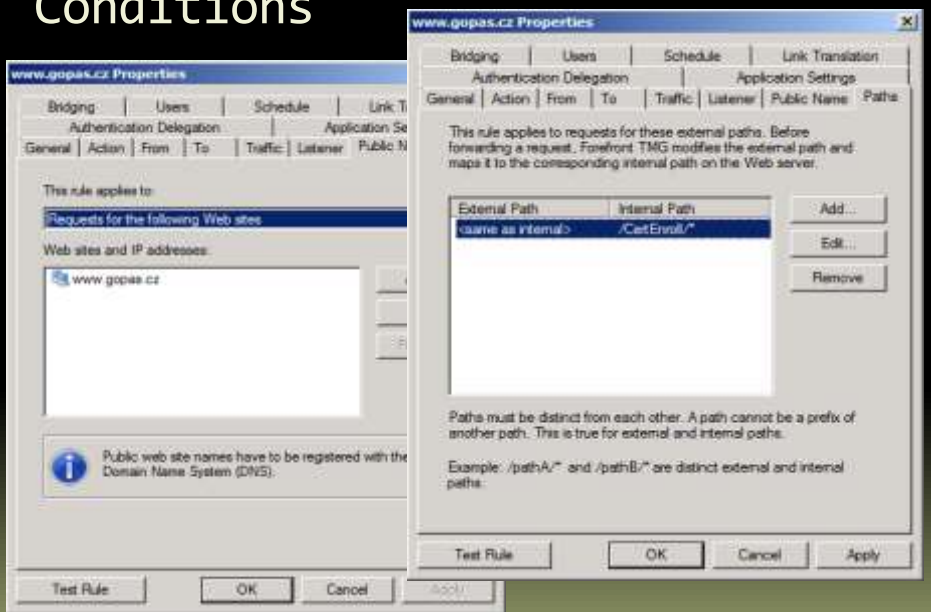
Web Server Publishing Rule

- Defines forwarding rules according to conditions met on the Web Listener
  - one listener – more publishing rules
- Conditions
  - Host header / URL asked for
- Forwarding
  - To which web server (IP or name)
  - With which host header
  - To which URL on the published web server

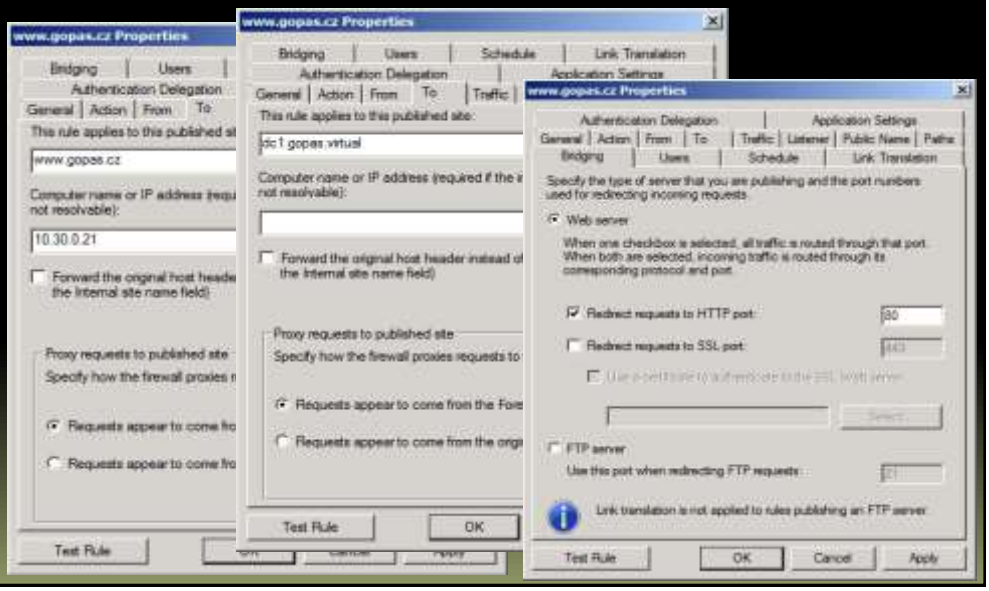
Conditions



Conditions



Published Web Site



Non authenticated

81.0.0.178	80
Public path	**Published path**
www.gopas.cz/*	10.30.0.21 internal host header www.gopas.cz
ca.gopas.cz/CertEnroll	GOPAS Root CA CRL dc1.gopas.virtual/CertEnroll

81.0.0.180	80
Public path	**Published path**
www.training-virtuosos.com/*	10.30.0.22 internal host header www.training-virtuosos.com

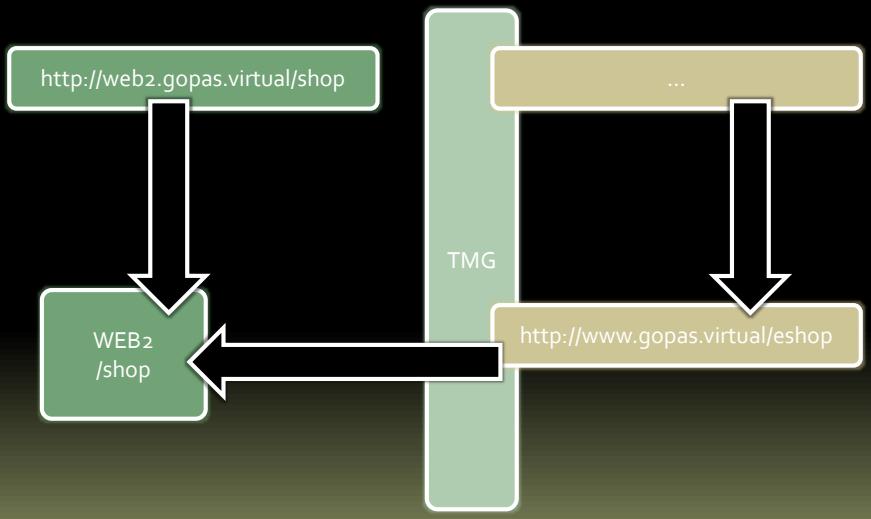
Lab

- Create two Web Listeners
  - HTTP 178, port 80, No authentication
  - HTTP 180, port 80, No authentication
- Publish sites according to the previous table
- Test access from WEB-EXT

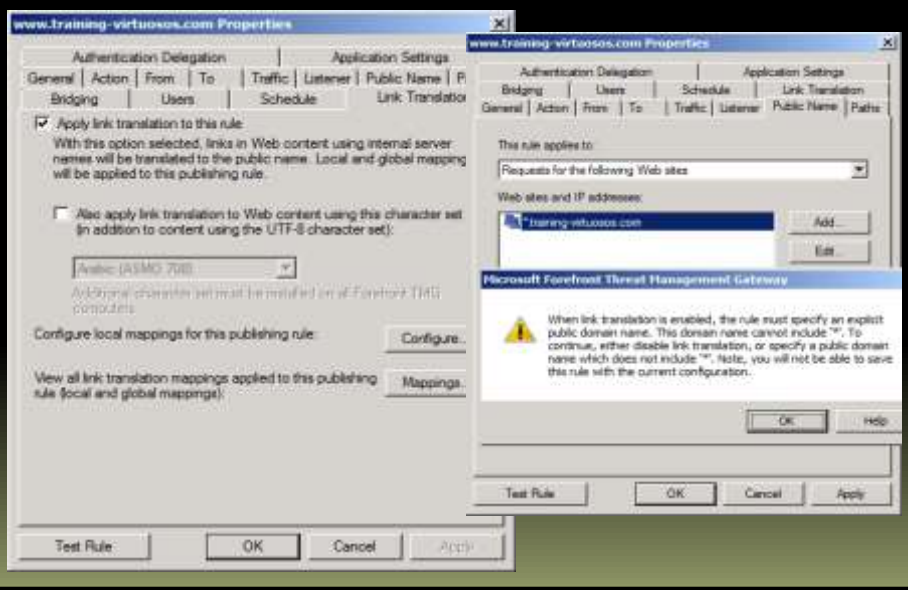
Link Translation

- TMG can replace links inside the published web pages when being returned to clients
  - automatic
  - explicit
- Public Name cannot use wildcards when Link Translation enabled

Link Translation



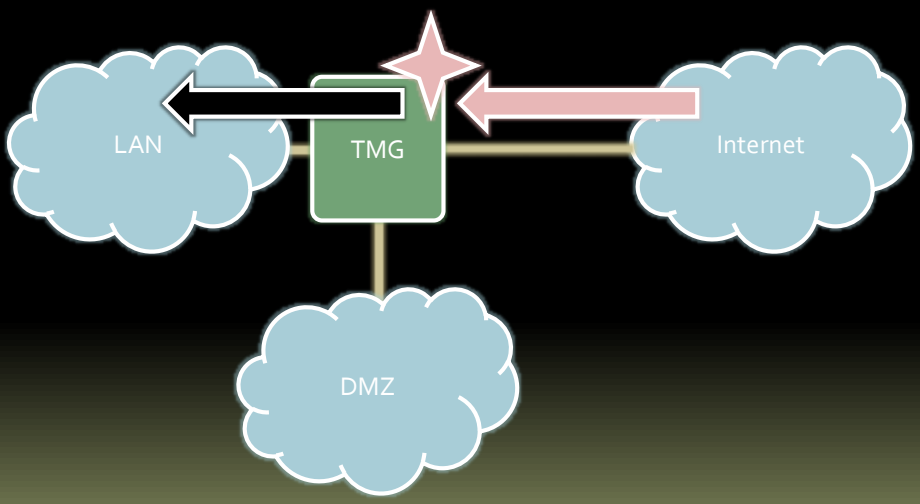
Link Translation



Threat Management Gateway 2010

AUTHENTICATION

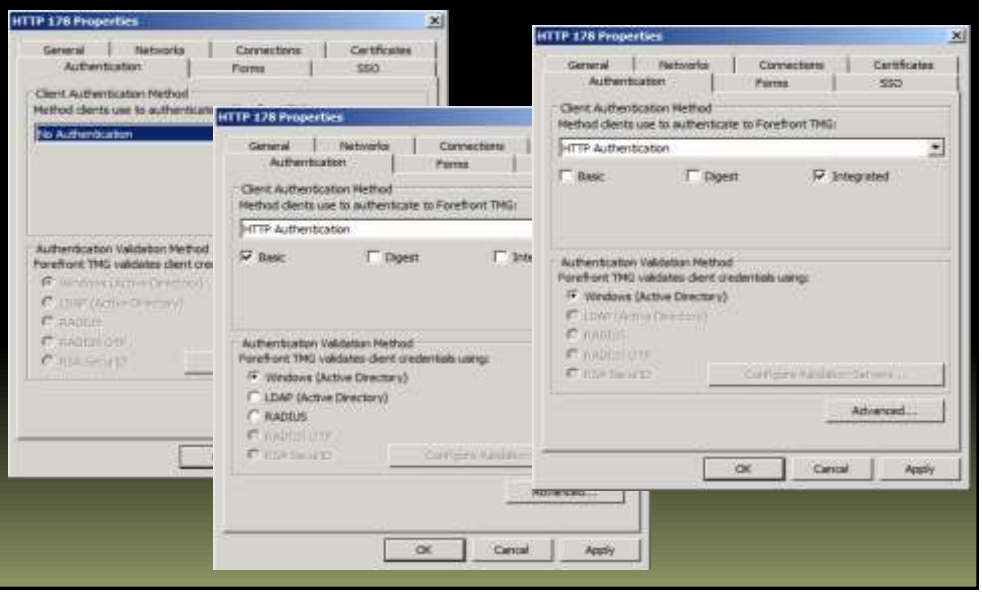
Web Listener Authentication



Web Listener Authentication

- Can have authentication enabled
  - if required, determined only later by a specific web server publishing rule
- HTTP Authentication
  - Basic/RADIUS, Windows, Digest
  - HTML Forms-Based
  - SSL Client Certificate

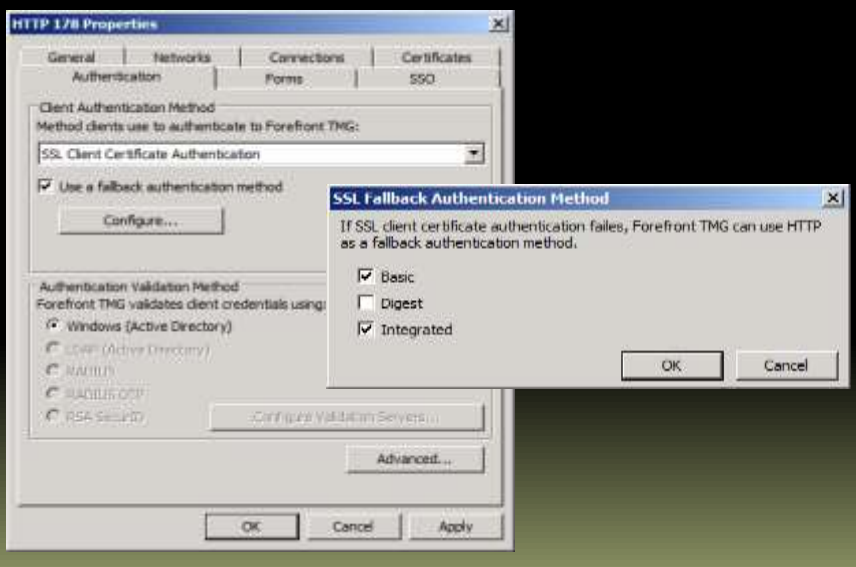
HTTP Authentication



HTTP Authentication

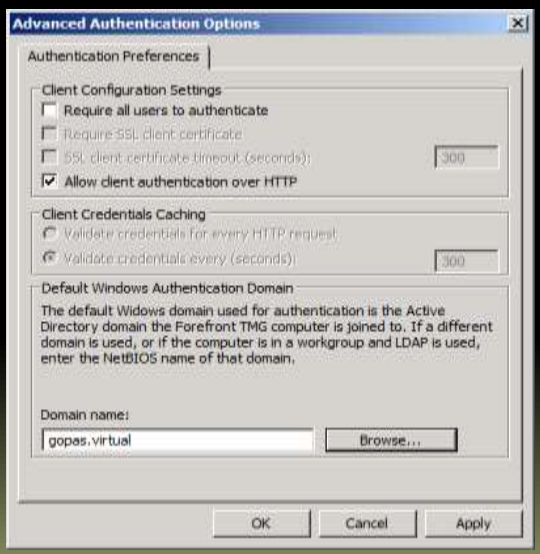
- Windows Integrated Authentication
  - WWW-Authenticate: Negotiate
  - WWW-Authenticate: Kerberos
  - WWW-Authenticate: NTLM
- NTLM only can be forced
  - KB927265
  - affects also Web Proxy

SSL Client Certificate



HTTP Authentication

- Must be enabled to be used over clear channel
- Remains in browser until process closed



Lab

- Enable HTTP Integrated Windows authentication on HTTP 180 web listener
  - enable authentication over clear-channel
- Modify training-virtuosos.com rule to require All Authenticated Users user set
- Test the access from WEB-EXT to verify that it requires domain authentication
  - at this point, the authenticated web page will not work yet (you need to wait for authentication delegation lesson)

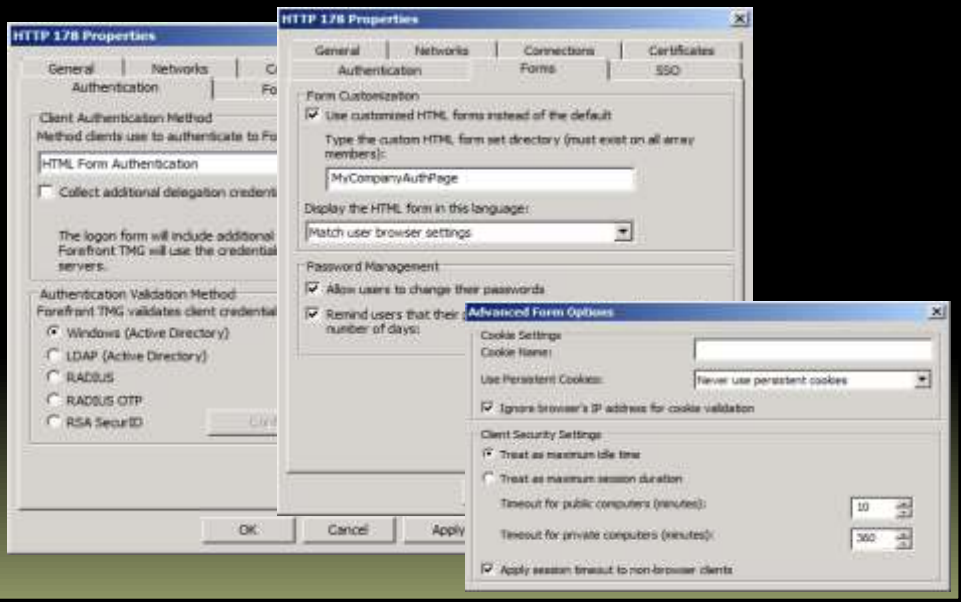
Threat Management Gateway 2010

FORMS AUTHENTICATION

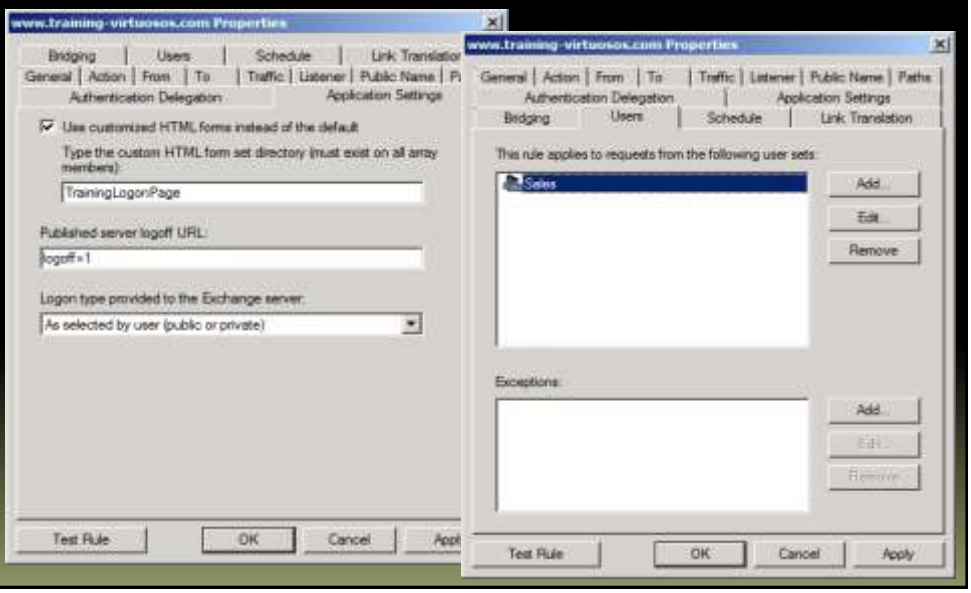
Forms-based Authentication

- Is not persistent in browser process
- Uses cookies on clients
- TMG stores session state in memory
  - expires after specified time of inactivity
- User can logoff
  - http://…/logoff=1
- Can be customized
  - %ProgramFiles%\Microsoft Forefront Threat Management Gateway\Templates\CookieAuthTemplates

Forms-based Authentication



Per Rule settings



Cookies and Forms

- Session cookies
  - persist only in the client browser process
  - expires according to TMG policy
- Persistent cookies
  - persist on disk of the client computer over browser restarts/logoffs
  - expires according to TMG policy

Forms fallback

- Only browser clients get the forms authentication
  - mobile devices get simpler format
- Non-browser clients fall back to Basic automatically
  - Windows Mobile ActiveSync, Autodiscover, Outlook Anywhere
  - fallback cannot use Windows Authentication
- User-Agent string mappings
  - google: Managing User-Agent Mappings

FBA Basic Fallback

No.	User-Agent headers	Authentication type
1	*Blazer*	XHTML-MP forms
2	*DoCoMo*	cHTML forms
3	*Windows CE*	XHTML-MP forms
4	*Symbain OS*	XHTML-MP forms
5	*SonyEricsson*	XHTML-MP forms
6	*Frontpage*	Basic authentication
7	*Mozilla*	HTML 4.01 forms
8	*Opera*	HTML 4.01 forms
9	*MSRPC*	Basic authentication
10	*	Basic authentication

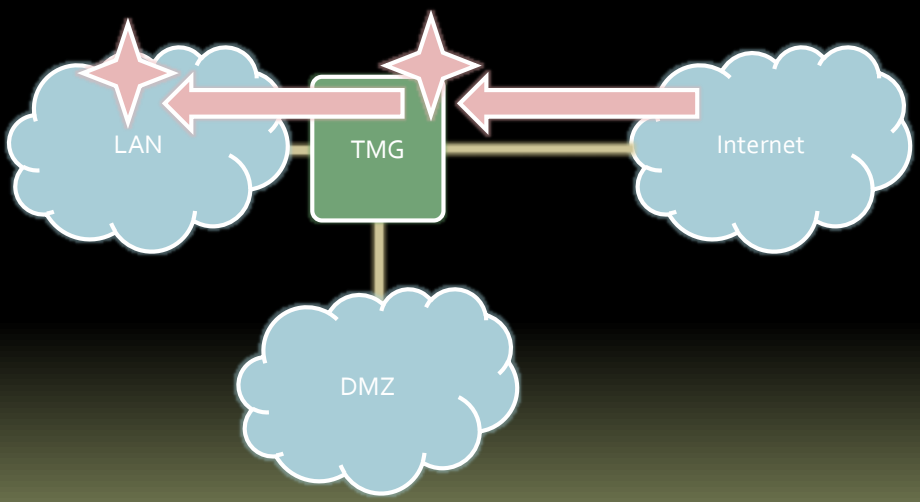
Lab

- Modify the HTTP 180 Web Listener to require Forms-based authentication
- Test the scenario from WEB-EXT
  - you can also try disabling cookies in IE
  - you can also try configuring logoff URL on the rule

Threat Management Gateway 2010

AUTHENTICATION DELEGATION

Authentication Delegation



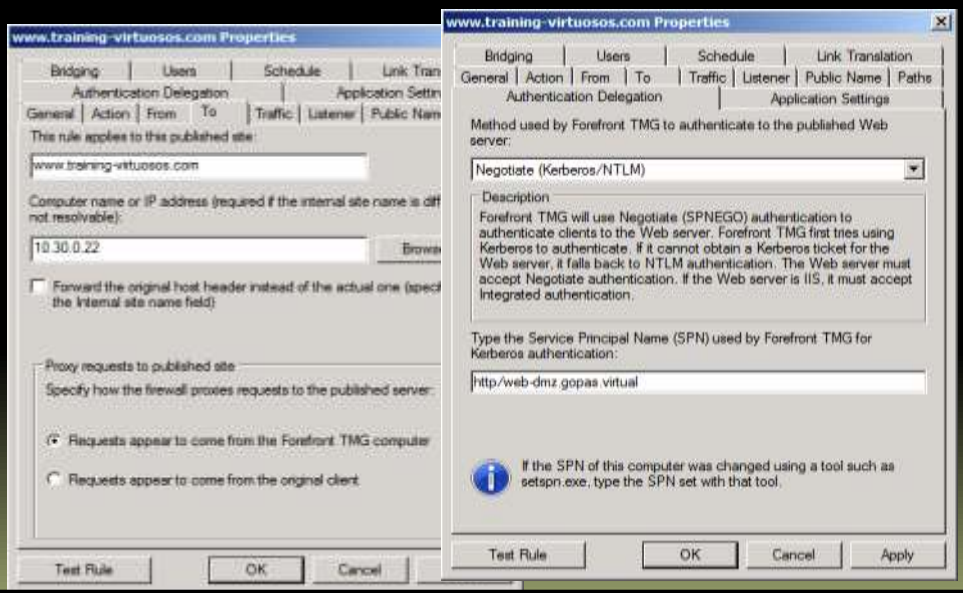
Authentication Delegation

- User provides login/password to the Web Listener
- Web Publishing Rule can forward the credentials to the backend published web site

Forwarding Options

Web Listener	Forwarding	Notes
Basic	all	TMG gets clear-text credentials
Forms		
Integrated	Kerberos Constrained Delegation	TMG does not get forwardable credentials TMG must be domain member Protocol Transition must be enabled in Active Directory
SSL Client Certificate		

Authentication Delegation



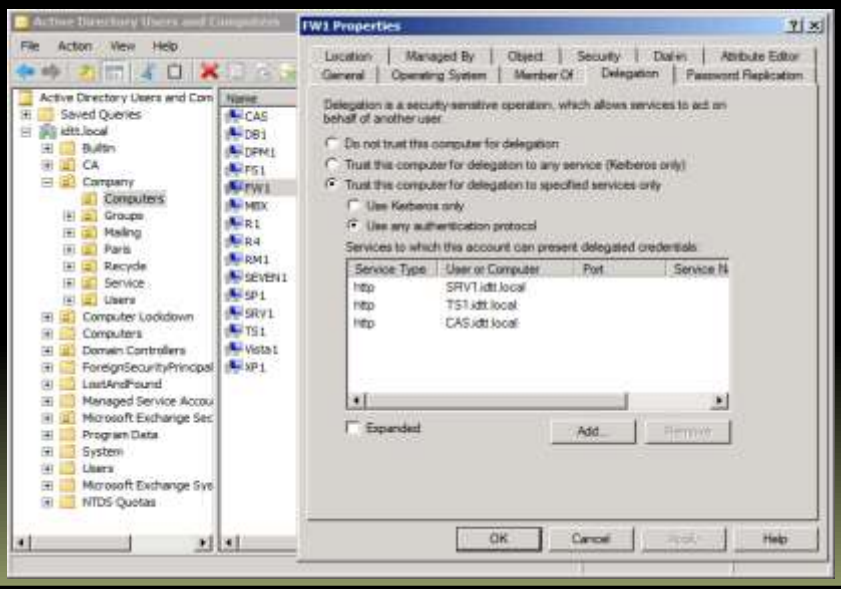
Lab

- Configure the training-virtuosos.com rule with Authentication Delegation to use Kerberos
  - don't use Keberos Constrained Delegation, it would require enabling Protocol Transition in AD
- Test the scenario from WEB-EXT
  - this time, the private authenticated page should be accessible

Protocol Transition

- TMG does not receive user credentials
  - Integrated Windows authentication
  - SSL Client Certificate
- Can logon the user anyway
  - without having anything in hand
  - Domain Admins must trust the firewall implementation

Protocol Transition

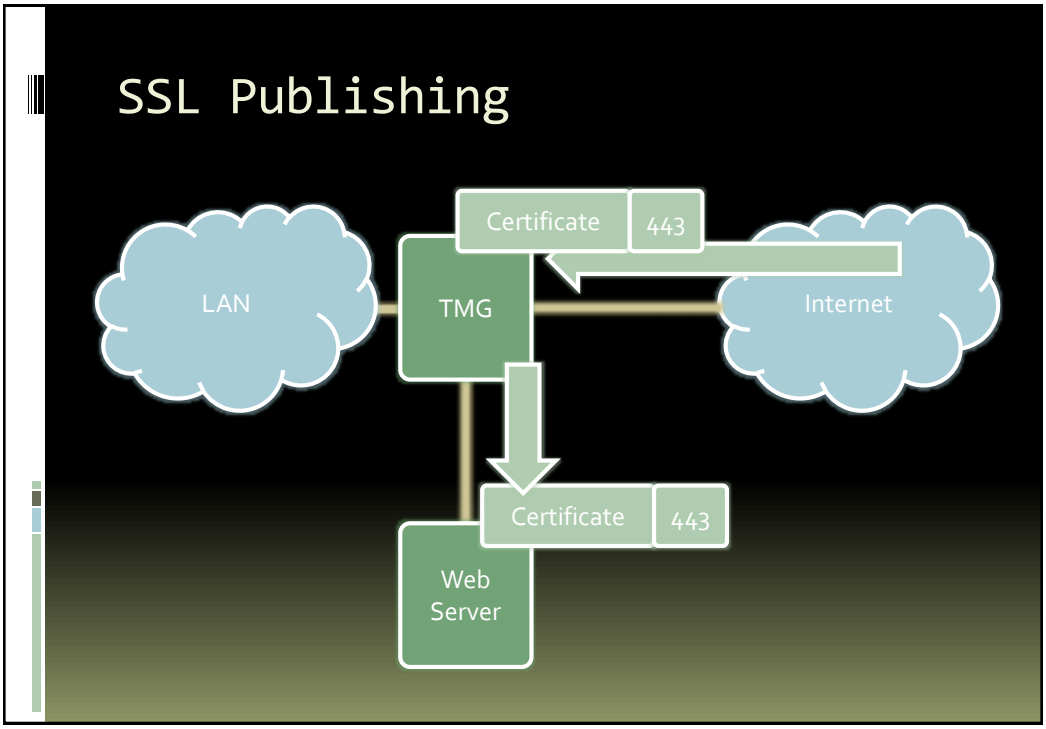


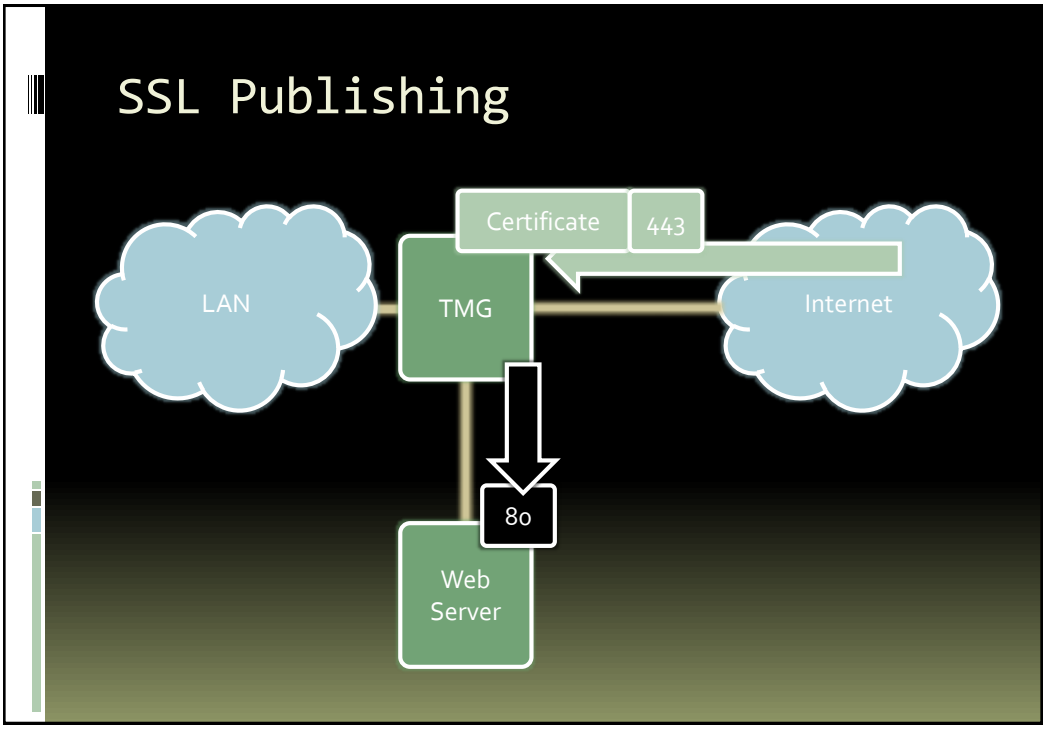
Lab: Optional

- Do this lab if you plan to implement SSL Client Certificate Logon later
- Enable the FW1 computer to be Trusted for Delegation to Any authentication protocol
  - FW1 must be restarted after
- Change the HTTP 180 Web Listener to require HTTP Integrated authentication
- Change the training-virtuosos.com rule to use the Kerberos Constrained Delegation as its Authentication Delegation mechanism
- Test the scenario from WEB-EXT
  - the private authenticated page should be still working

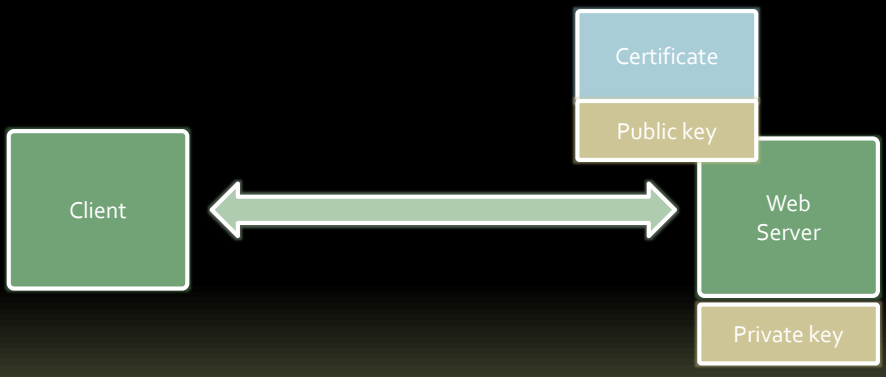
Threat Management Gateway 2010

SSL PUBLISHING

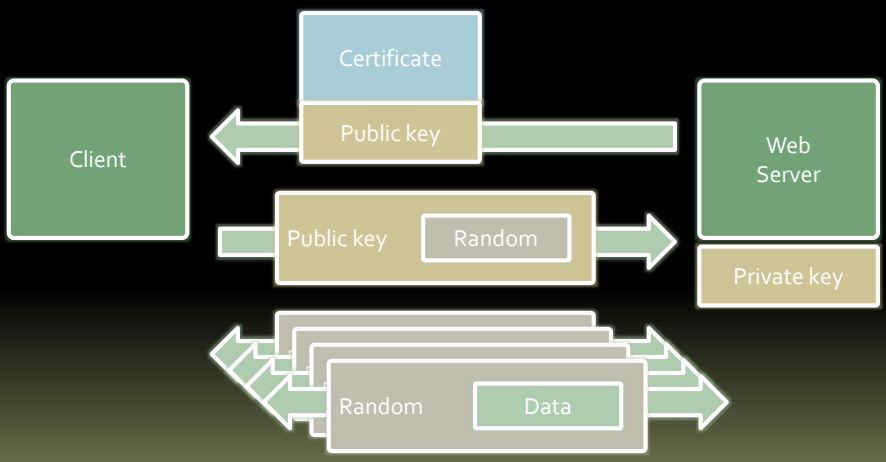

SSL Publishing
LAN
TMG
Certificate
443
Internet
Certificate
443
Web
Server


SSL Publishing
LAN
TMG
Certificate
443
Internet
80
Web
Server

Secure Socket Layer



Secure Socket Layer



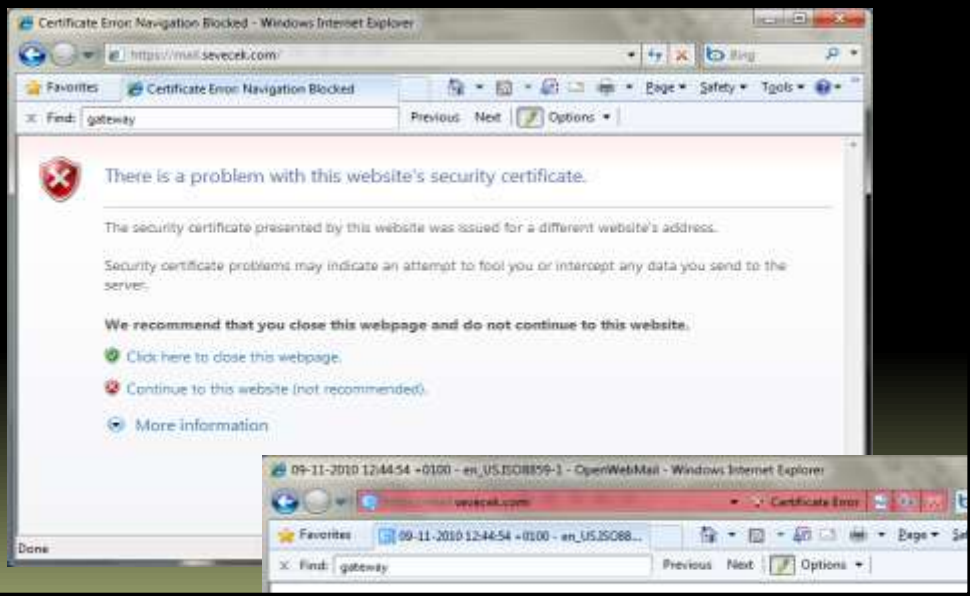
Server Certificate

- Subject
  - www.gopas.cz or *.gopas.cz
- Subject Alternative Name (SAN)
  - can contain more names
- Enhanced Key Usage (EKU) and Application Policies (AP)
  - Server Authentication

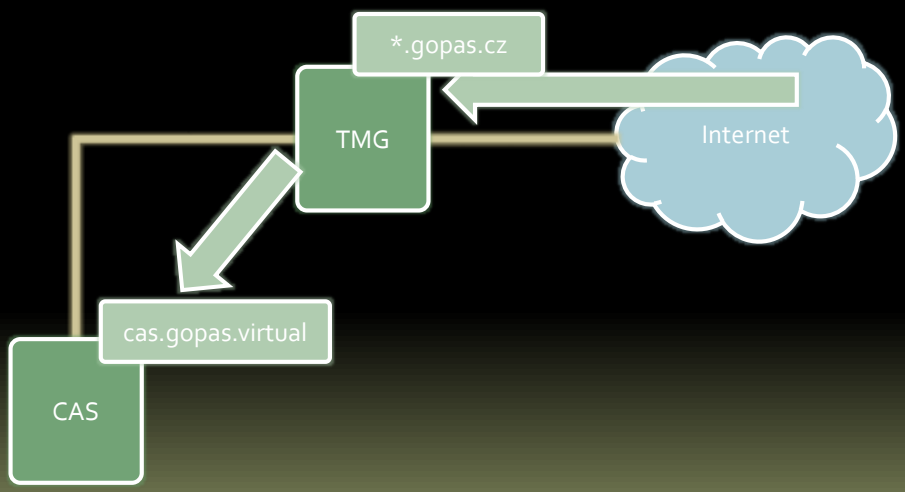
Certificate Validation

- Subject/Name
  - Windows Mobile 5.0 and older browsers do not support wildcards
- Issuing authority
  - must be trusted
- Validity dates
- Certificate Revocation List (CRL)
  - must be accessible from outside on HTTP path

Invalid Certificate



Certificate Subject



Certificate Enrollment

- Private CA
  - Certificate Services with Enterprise CA type
  - is trusted automatically on domain member computers
- Public CA
  - costs money
  - is trusted automatically on lots of devices

SSL Certificate Prices (per name)

- Verisign – 1999
  - 300$ year
- Thawte – 2003
  - 150$ year
- Go Daddy – 2005
  - 30$ year
- GlobalSign – 2006
  - 250$ year
- StartCom – 2009
  - free

Video/Pictures

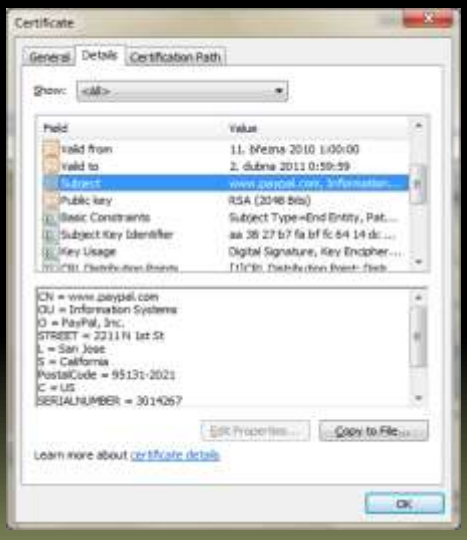
- Phishing-with-Valid-Certificate

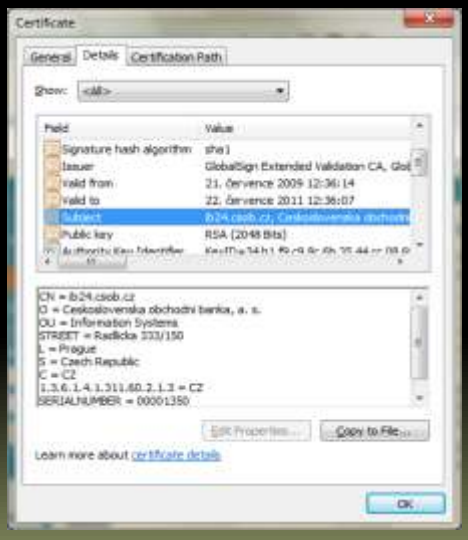
Extended Validation Certificates (green bar)

- CA validates the real identity of the owner of the domain
  - not just the domain name registration
- Ensures postal/legal address is present in the certificate
  - Street, City, Country, Business Registration Number (IČO)
- Examples
  - http://www.paypal.com
  - http://www.servis24.cz

EV Certificates

Certificate Subject





EV Certificate Prices (per name)

- Verisign – 1999
  - 1500$ year
- Thawte – 2003
  - 600$ year
- Go Daddy – 2005
  - 100$ year
- GlobalSign – 2006
  - 900$ year
- StartCom – 2009
  - 50$ year

EV browsers

Browser	Version
Internet Explorer	7.0
Opera	9.5
Firefox	3
Google Chrome	-
Apple Safari	3.2
Apple iPhone	3.0

SSL Web Listener

- Only single certificate per IP address
- Cannot use Host headers unless used with wildcard certificate
  - Example: *.gopas.cz
- The certificate must be present in the Local Computer store and must be valid and completely trusted (including CRL)
  - TMG does not support v3 Templates

SSL Web Listener

Lab

- If you plan to use web enrollment, make sure you can open http://dc1/CertSrv from FW1
  - you may need to create a new access rule for it
- By using the Web Enrollment Pages or MMC / Certificates / Local Computer create three separate requests for *.gopas.cz, mobile.gopas.cz and *.training-virtuosos.com certificates
  - if you want to fill the SAN extension as well, use the attributes edit box and type something like "SAN:dns=*.gopas.cz"
- After uploading the requests using the web application, switch to DC1 and using the Certificate Authority console, Issue the certificates
  - you may need to Publish CRL first

Lab

- Back on the FW1 download and install the issued certificates from the authority
- Start MMC and Add Snap-in for both Certificates (Current User) and Certificates (Local Computer)
- Export all the three certificates with private keys from the user store and import them back into local computer store
  - don't use drag-and-drop!

Lab

- Create four separate Web Listeners for each certificate
  - HTTPS gopas.cz 178, Basic authentication
  - HTTPS gopas.cz 179 , Basic authentication
  - HTTPS training-virtuosos.com 180 , Basic authentication
  - HTTPS mobil.gopas.cz 181, Basic authentication

Threat Management Gateway 2010

SAMPLE PUBLISHING

Sample Publishing

- The following tables show sample publishing combinations in the most secure manner possible
- The SSL Client Certificate authentication can be replaced by any other authentication
  - but would be most secure if implemented

Authenticated with Client SSL certificate (*.gopas.cz)

81.0.0.178	443

Public path	Published path
mail.gopas.cz/ecp	OWA Settings cas.gopas.virtual/ecp
mail.gopas.cz/*	OWA cas.gopas.virtual/owa
portal.gopas.cz/*	SharePoint 2010 sp.gopas.virtual
ts.gopas.cz/rpc	RDS Gateway ts.gopas.virtual/rpc
ts.gopas.cz/*	RDS Web Access policy.gopas.virtual/RDWeb

Authenticated with password (*.gopas.cz)

81.0.0.179 443

Public path	Published path
rpc.gopas.cz/rpc	Outlook Anywhere cas.gopas.virtual/rpc
gopas.cz/Autodiscover autodiscover.gopas.cz/Autodiscover	Audodiscover cas.gopas.virtual/autodiscover
vpn.gopas.cz	SSTP VPN authentication setting ambiguous

Authenticated with Client SSL certificate (*.trining-virtuosos.com)

81.0.0.180 443

Public path	Published path
www.training-virtuosos.com/Private	10.30.0.22/Private internal host header www.training-virtuosos.com

Authenticated with password or SSL Client Certificate (mobile.gopas.cz)

81.0.0.181	443
Public path	**Published path**
mobile.gopas.cz/Microsoft-Server-ActiveSync	cas.gopas.virtual/Microsoft-Server-ActiveSync

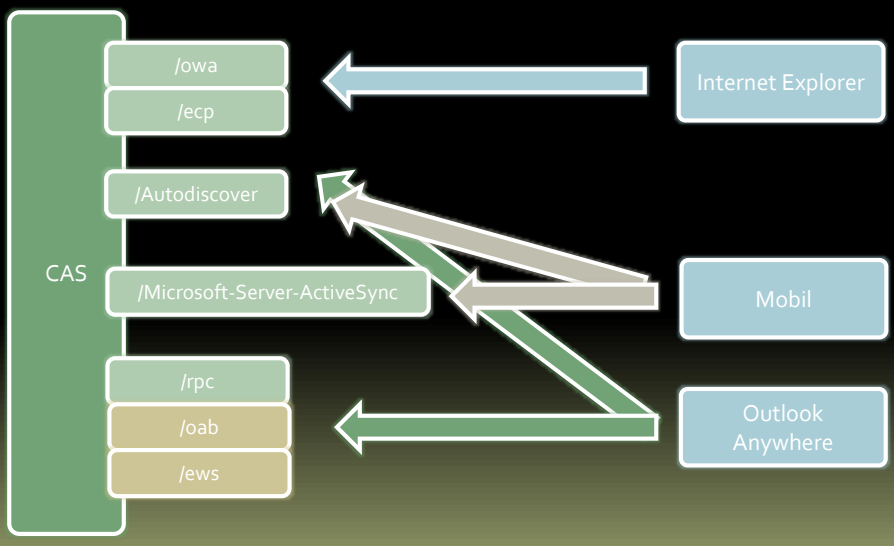
Lab

- Implement and test the sample publishing for www.gopas.cz and www.training-virtuosos.com from previous tables with Basic authentication
  - the rest will come later ☺
- Optional: If you like, you can switch then the authentication to SSL Client Certificate, issue the GOPAS Logon Certificate to a user of Seven1 and test the scenario from Internet location

Threat Management Gateway 2010

EXCHANGE SERVER NOTES

HTTPS Klienti



Authentication

- OWA/EWS
  - any authentication suitable for users
- ActiveSync
  - basic, forms (with fallback), SSL certificate
  - cannot use Windows Integrated
- Outlook Anywhere
  - basic, windows, forms (with fallback)
  - cannot use SSL certificates
- RDP/TS Gateway
  - windows, SSL certificates
  - basic and forms (with fallback) when enabled in GPO

Exchange server certificate

- Internal client access done always to the real CAS name
  - https://cas.gopas.virtual/…
- External client access over port forwarding
  - POP3, SMTP, IMAP
  - No SSL inspection, directly accessing the backend CAS server
  - *.gopas.cz

Exchange server certificate

- Get-ExchangeCertificate | fl
- Enable-ExchangeCertificate -Thumbprint -Services <None | IMAP | POP | UM | IIS | SMTP | Federation>
  - IMAP, POP, IIS – certificate needed on CAS
  - SMTP – certificate present on MBX

Exchange external access

- OWA and ECP
  - Set-OwaVirtualDirectory
    -ExternalUrl https://mail.gopas.cz/owa
    -BasicAuthentication $false
    -DigestAuthentication $false
    -FormsAuthentication $false
    -WindowsAuthentication $true
  - Set-EcpVirtualDirectory
    -ExternalUrl https://mail.gopas.cz/ecp
    -…

Exchange external access

- ActiveSync
  - Set-ActiveSyncVirtualDirectory
    -ExternalUrl https://mobile.gopas.cz/Microsoft-Server-ActiveSync
    -ExternalAuthenticationMethods Certificate
    -InternalAuthenticationMethods WindowsIntegrated
    -ClientCertAuth Ignore

Exchange external access

- Outlook Anywhere (RPC over HTTP)
  - Enable-OutlookAnywhere
    -ClientAuthenticationMethod NTLM
    -IISAuthenticationMethods NTLM
    -ExternalHostName rpc.gopas.cz
    -SslOffloading $false
- EWS
  - Set-WebServicesVirtualDirectory
    -ExternalUrl https://mail.gopas.cz/ews
    -BasicAuthentication $false
    -CertificateAuthentication $false
    -DigestAuthentication $false
    -WindowsAuthentication $true
- OAB
  - Set-OabVirtualDirectory
    -ExternalUrl https://mail.gopas.cz/oab
    -BasicAuthentication $false
    -WindowsAuthentication $true

Exchange external access

- Autodiscover
  - 1) https://gopas.cz/Autodiscover
  - 2) https://autodiscover.gopas.cz/Autodiscover
  - 3) SRV _autodiscover._tcp.gopas.cz, TCP 443
- Set-AutodiscoverVirtualDirectory
  -ExternalUrl
  https://autodiscover.gopas.cz/Autodiscover/Autodiscover.xml
  -BasicAuthentication $false
  -DigestAuthentication $false
  -WindowsAuthentictation $true
- Set-OutlookProvider
  -CertPrincipalName "msstd:*.gopas.cz"
  - the name in the public certificate

Autodiscover SRV

- As last the resort after direct HTTPS trials
- Single-name certificates
- Not supported by some mobile phones (Windows Mobile 5.0-, iPhone 4-)

Disable Autodiscover

- Have public DNS zone resolvable both from internal as well as external network
  - gopas.cz
- Do not define DNS names
  - autodiscover…
  - _autodiscover._tcp…
- Do not publish /Autodiscover/*

Troubleshooting: Kerberos

- IIS config gets sometimes corrupted ☺
- %WINDIR%\System32\inetsrv\Config
  - applicationHost.config

```
<windowsAuthentication enabled="true"
   useKernelMode="false">
    <provider>
      <clear/>
      <add value="Negotiate"/>
      <add value="Ntlm"/>
    </provider>
</windowsAuthentication>
```

Lab

- On CAS and MBX by using MMC and the Certificates (Local Computer) console enroll for
  - GOPAS Domain Server certificate template
    - this certificate is going to be used for IIS
  - GOPAS Web Server and set the Subject to mail.gopas.cz
    - the certificate is going to be configured for SMTP, POP and IMAP
- Assign the newly created certificate to the IIS OWA web site
  - Get-ExchangeCertificate
  - Enable-ExchangeCertificate -Services IIS
- Assign the other certificate to the SMTP, POP and IMAP services
  - Enable-ExchangeCertificate -Services POP, IMAP, SMTP
- Test the HTTPS://cas.gopas.virtual/owa local connectivity

Lab

- Configure public URLs on CAS for all the services
- Change the OWA authentication to Windows Integrated
  - test again the local network access
- Publish the OWA access by using the sample publishing rules from previous lesson

Threat Management Gateway 2010

ADVANCED EXCHANGE TOPICS

Recommended HTTP Inspection

- Demo folder:
  - Exchange-Publishing-HTTP-Filter
- or Google
  - Typical HTTP Policies for Web and Outlook Web Access Publishing Rules

Blocking Cross-Site-Scripting

- Example:
  - when a user post a script into a newsgroup
- Block <SCRIPT> tags in requests
  - block %3C%73%63%72%69%70%74%3E as well (ASCII encoded version)

Blocking Cross-Site-Scripting

- Block others
  - but be careful

ActiveXObject	DeleteFile	GetSpecialFolder	OnChange	OnLoad	OnResize
applet	DriveType	javascript	OnClick	OnMouseDown	OnSelect
cookie	EMBED	livescript	OnDragDrop	OnMouseMove	OnSubmit
CopyFile	FileExist	mocha	OnFocus	OnMouseOut	OnUnload
copyparentfolder	GetFile	object	OnKeyDown	OnMouseOver	OpenAsTextStream
CreateObject	GetFolder	OnAbort	OnKeyPress	OnMouseUp	OpenTextFile
CreateTextRange	GetParentFolder	OnBlur	OnKeyUp	OnMove	RegWrite
Replace	SCRIPT	vbscript			

Troubleshooting Outlook

- Test E-mail AutoConfiguration
  - notification icon, CTRL + right-click
- Force Autodiscover to rebuild profile settings
  - automatically every 6 hours
  - Tools / Account Settings / Repair…

Autodiscover

- Outlook and Windows Mobile can use SRV record _autodiscover
  - can point to something like mail.gopas.cz
  - the SSL certificate can have just a single name for all services
- iPhone does not use the SRV record and requires autodiscover.gopas.cz name
  - SSL certificate should have this name inside

External Exchange SMTP

- HELO/EHLO welcome banner on Edge Transport
- Set-ReceiveConnector -Fqdn
- Set-SendConnector -Fqdn

Lab

- Configure Edge Transport receive connector with appropriate FQDN
  - Set-ReceiveConnector –Fqdn mail.gopas.cz
  - Set-SendConnector –Fqdn mail.gopas.cz

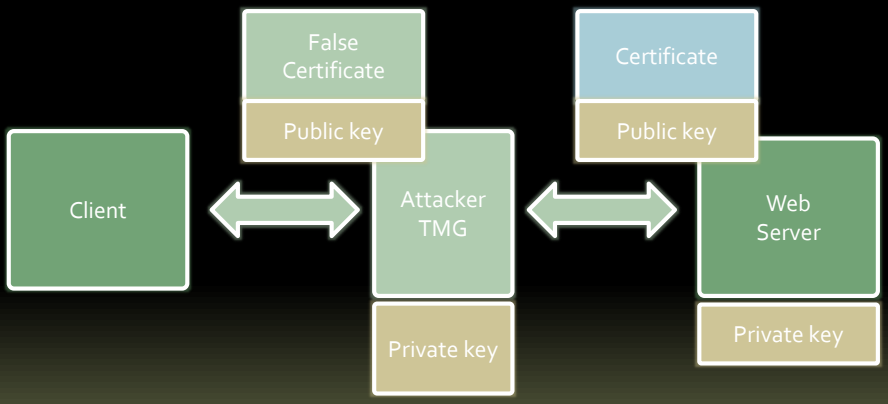
Threat Management Gateway 2010

FORWARD SSL INSPECTION

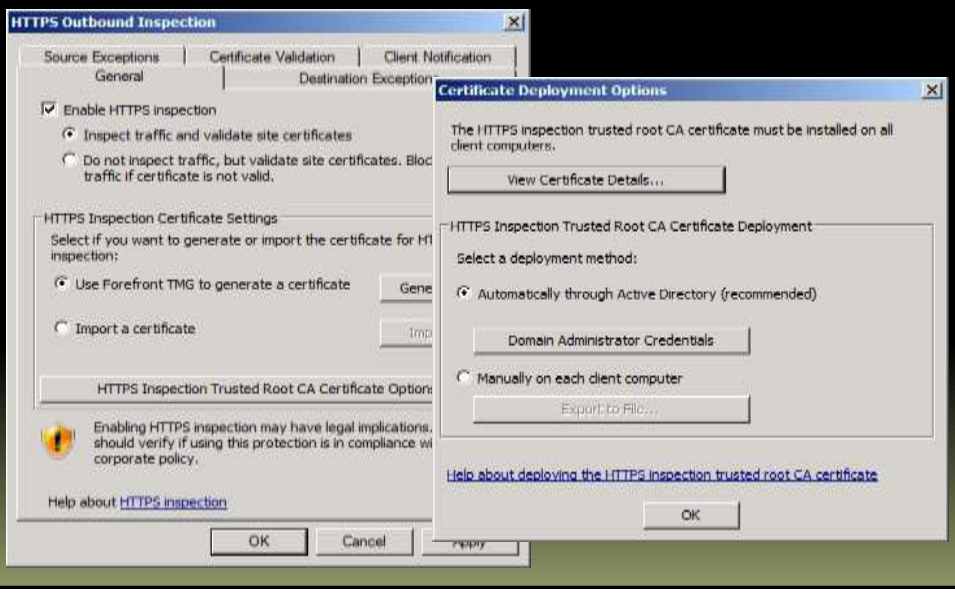
Forward SSL Inspection

- TMG can perform MITM (Man in the Middle) attach on the forward SSL traffic to be able to inspect it
- The forged certificates can be made trusted on the clients

Attacking SSL

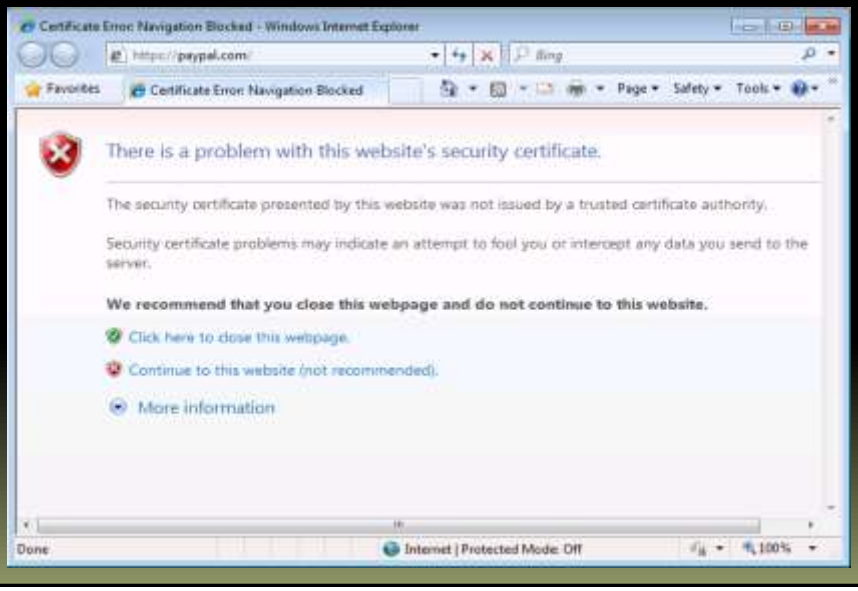


Forward SSL Inspection

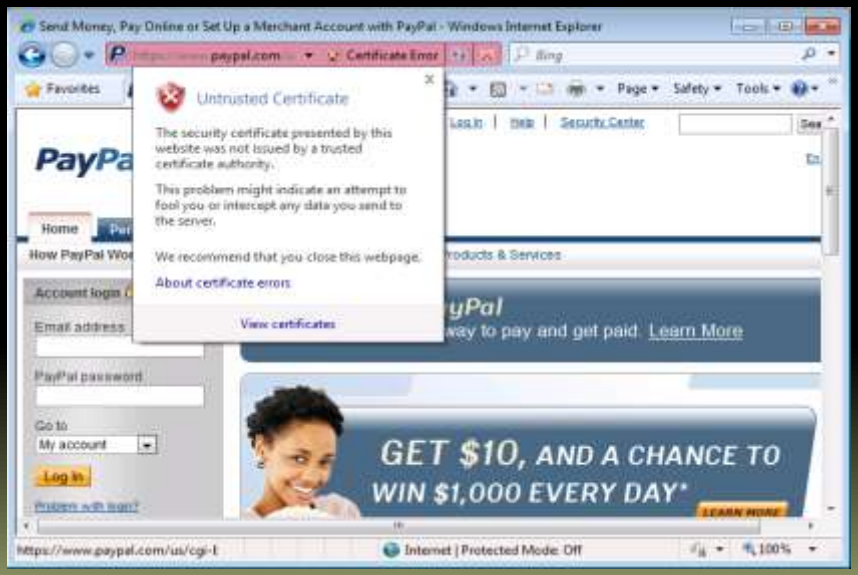


No SSL Inspection

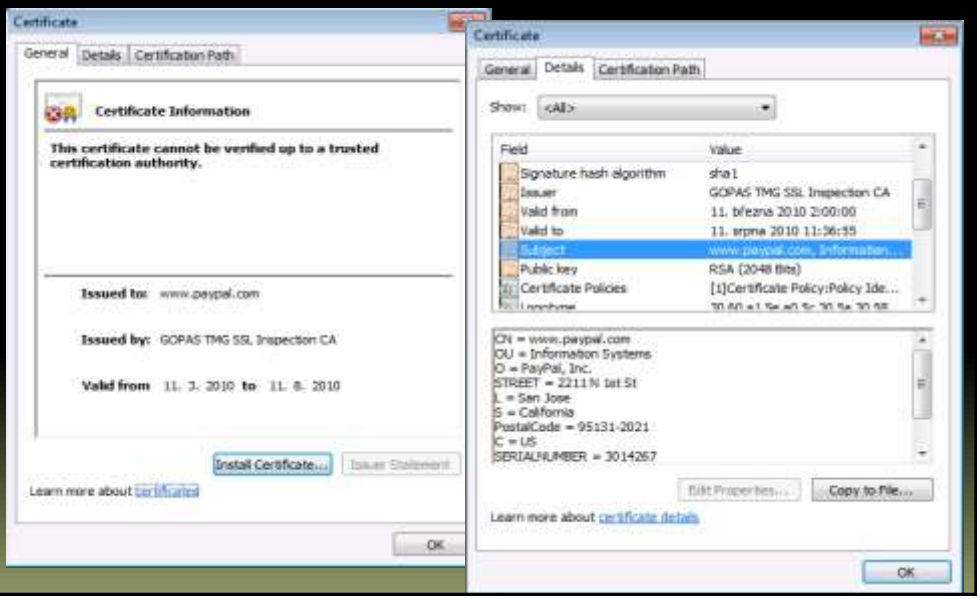
TMG CA Not Trusted



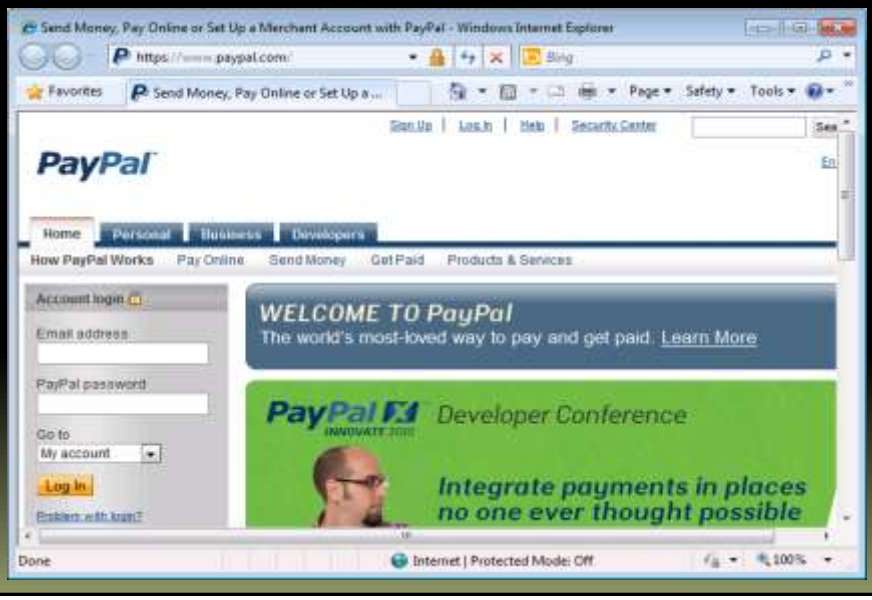
TMG CA Not Trusted



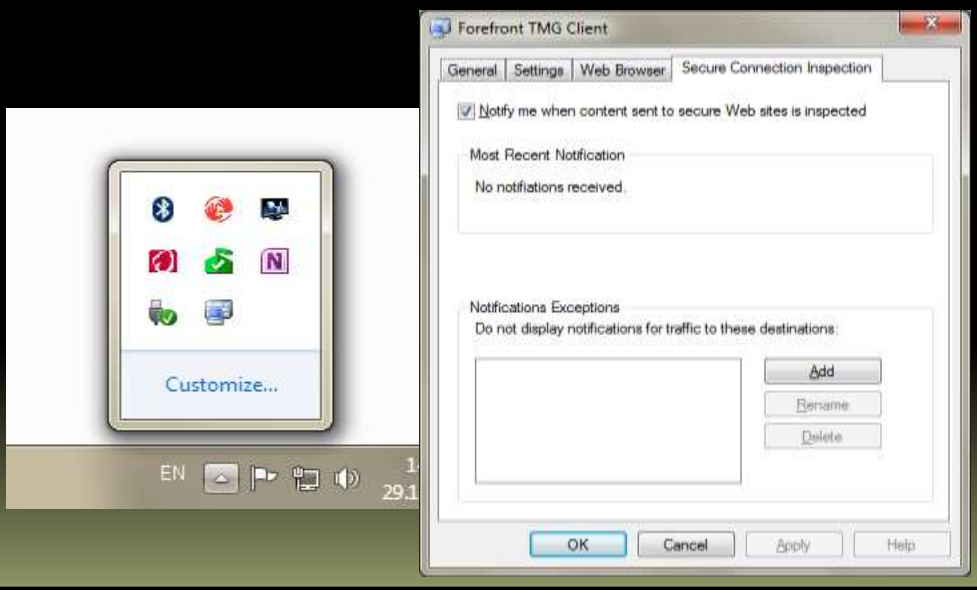
Web Server Certificate



TMG CA Trusted on the Client



TMG Client Notification



Lab

- Enable forward SSL inspection
- Try accessing https://paypal.com from DC1
  - this should be with an error message and red address bar
- Make the TMG issuer trusted in Active Directory
- On DC1 issue CERTUTIL -PULSE command
  - this is to update the trusted root CA list
- Try again the web access
  - this time without any error with white address bar
- Look at the web site false certificate and compare it with its original one
  - note that the original address bar is green

Ondřej Ševeček | GOPAS a.s. |
MCM: Directory Services | MVP: Enterprise Security |
ondrej@sevecek.com | www.sevecek.com |

THANK YOU