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

VPN

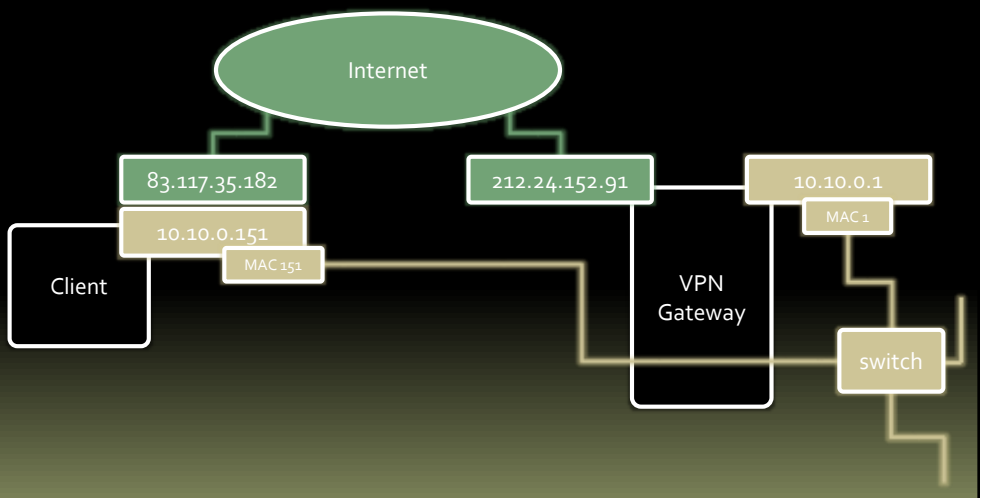
Threat Management Gateway 2010

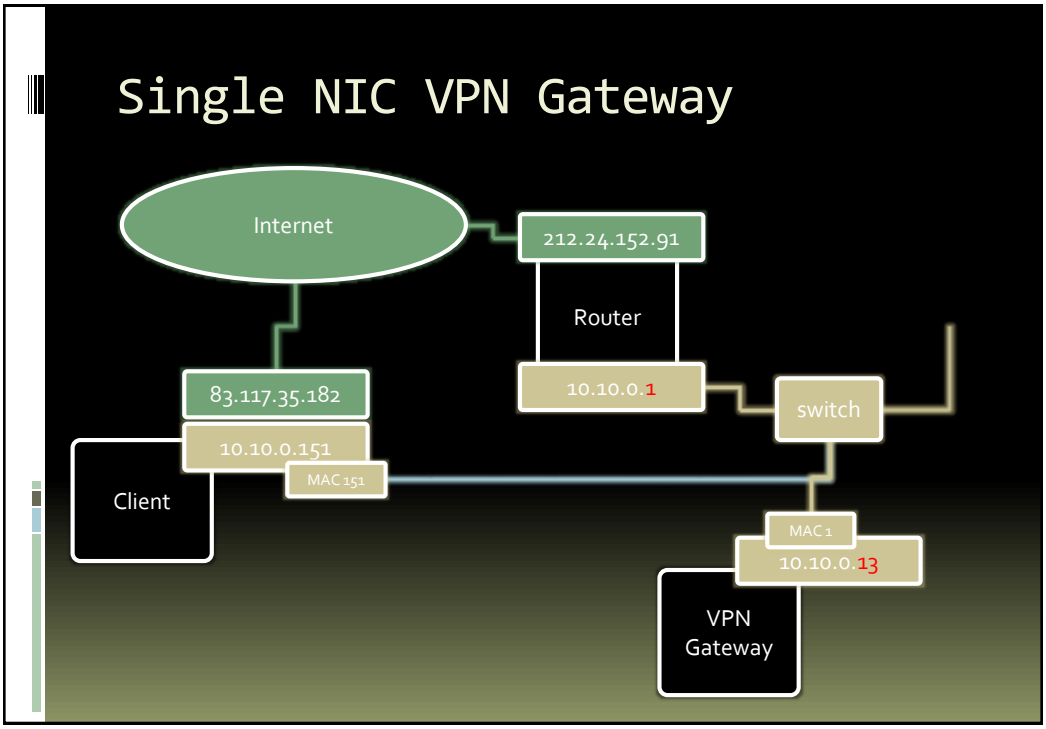
VIRTUAL PRIVATE NETWORKING

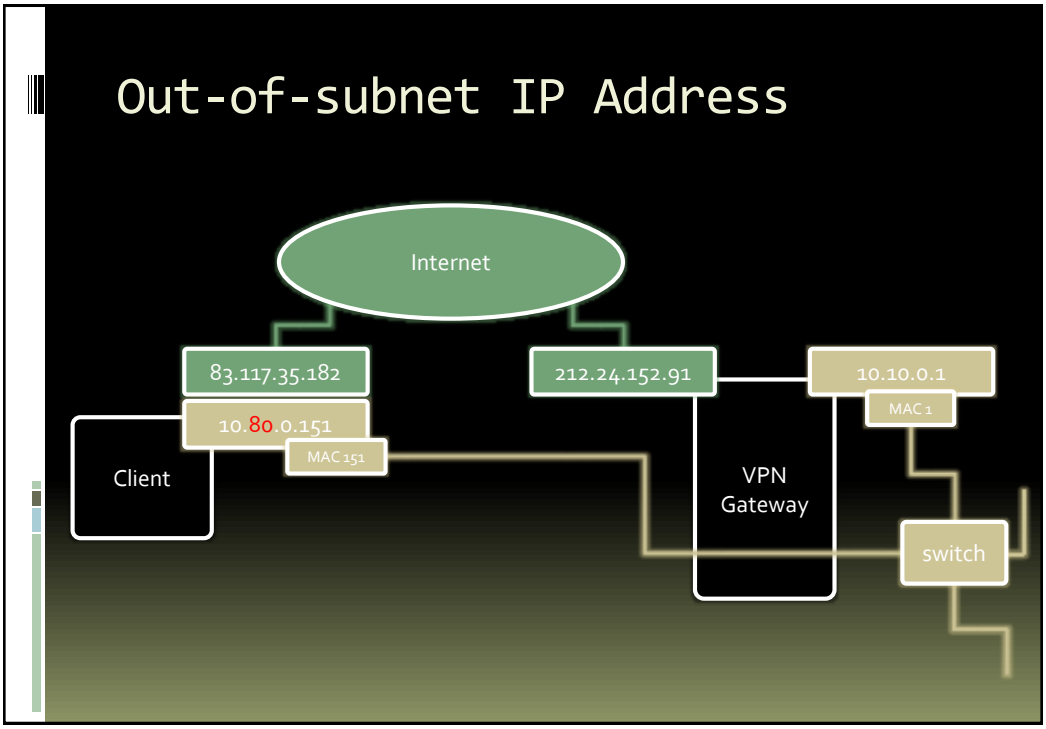
What is VPN?

- Remote connection over internet
- Authentication
  - User, sometimes computer authentication
- Encryption
- Private IP address assignment
  - not necessary with DirectAccess
- Quarantine
  - if required

IP Address Assignment




Single NIC VPN Gateway
Internet
212.24.152.91
Router
10.10.0.1
switch
83.117.35.182
10.10.0.151
MAC 151
Client
MAC 1
10.10.0.13
VPN
Gateway


Out-of-subnet IP Address
Internet
83.117.35.182
10.80.0.151
MAC 151
Client
212.24.152.91
VPN
Gateway
10.10.0.1
MAC 1
switch

Microsoft VPN

- Clients available on wide range of OS
- Private IP address assignment
  - some hardware VPNs do not assign private IP addresses and clients appear as public to internal servers
- Simple to use authentication with Active Directory accounts
  - others must use RADIUS or LDAP

VPN with TMG

- Is not itself a VPN server at all
- Configures RRAS as VPN server
  - you should not use the RRAS GUI at all
- Inspects the traffic only after decryption
  - can look inside completely as it was an intranet client

Threat Management Gateway 2010

CONNECTION SELECTION

Client Connections

VPN	Connection requirements	Logon	Client Availability	Authentic.
RDP	TCP 3389 server certificate (not required)	random keys (D-H) certificate private key (2048bit)	Windows XP	password smart card
RDS/TS Gateway	TCP 443 server certificate	random keys (D-H) certificate private key (2048bit)	Windows XP	password smart card
PPTP	GRE + TCP 1723	depends on password quality vulnerable to offline cracking	MS-DOS	password smart card
L2TP	IPSec ESP + UDP 500/4500 server certificate client computer certificate	random keys (D-H) certificate private key (2048bit)	Windows 98	password smart card
SSTP	TCP 443 server certificate	random keys (D-H) certificate private key (2048bit)	Windows Vista	password smart card

Link Characteristics

- Bandwidth
  - x Mbps
  - determines the speed of large up/downloads
- Latency (Round-Trip Time)
  - x ms
  - determines the speed of small downloads
  - affects "talky" protocols
- Packet Loss Rate
  - 1/n
  - often appear in chunks
  - affects double tunneled connection oriented protocols

SMB/CIFS/RPC/DCOM/SQL

- Talky protocol
- Require a lot of round-trips to transfer even small data
  - problematic/slow with latency higher than 50ms
- Do not require high bandwidth

Tunneling TCP

- TCP acknowledges every sent packet
  - retransmitted if lost in transmit
- PPTP and SSTP both do it as well
  - sensitive to packet loss
  - single packet loss generates several retransmissions on both layers
- IPSec do not use acknowledgements
  - better for TCP transmissions

Remote Access Recommendations

- Don't access SMB/CIFS/RPC/DCOM/SQL over latent links
  - use RDP instead
- Don't runnel TCP over PPTP/SSTP over high packet loss links
  - use RDP Gateway instead
  - use IPSec tunnel for site-to-site VPNs

VPN Security

- Usually opens full network access into internal network
- Usually can be dialed from insecure computers
  - home computers
  - internet cafes

VPN Security

- Decide whether VPN required at all
  - Use RDP Gateway instead
- Use L2TP to enforce client computer certificates
  - limits connections from non-corporate machines
- Implement VPN Quarantine or Network Access Protection
  - improves the health of network

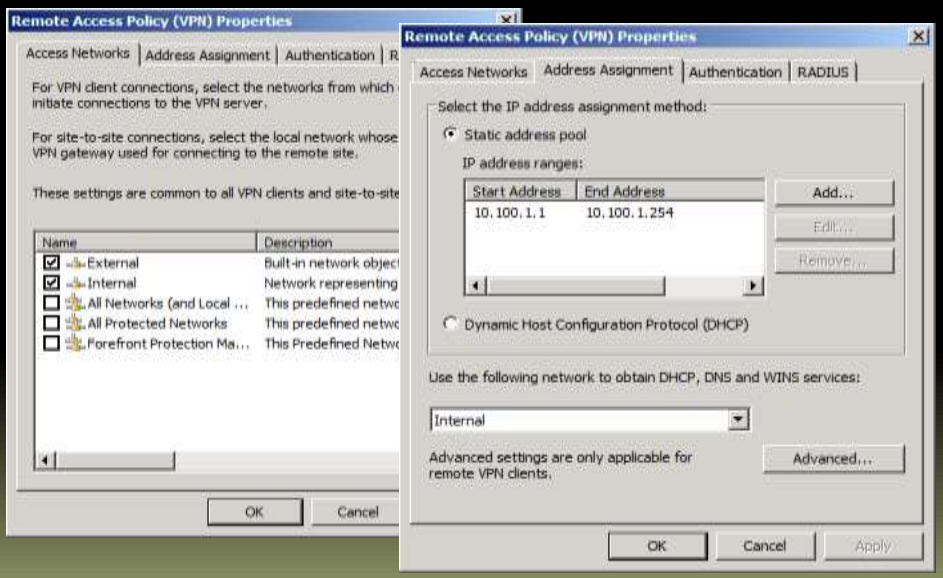
Threat Management Gateway 2010

VPN CONFIGURATION

Windows 2008 RRAS

- Local RRAS and NPS
  - should not be configured directly
  - not supported
- Can do only what is configured inside TMG GUI console
- If you need more granular control and functionality, use remote NPS

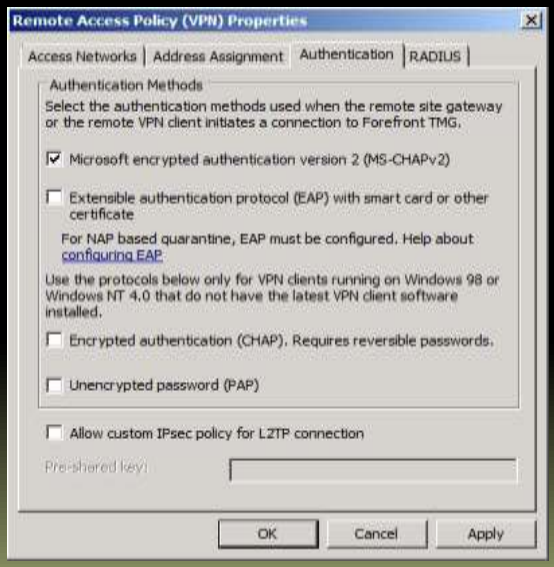
Step 1 and 2



Password Authentication

- MS-CHAPv2
  - uses Microsoft NTLM hashes (MD4)
  - clients at least Windows 95+
- Transferred inside the tunnel
  - When used with PPTP, the hashes are visible
  - Other VPNs encrypt them with own cryptography
- Vulnerable to keyloggers

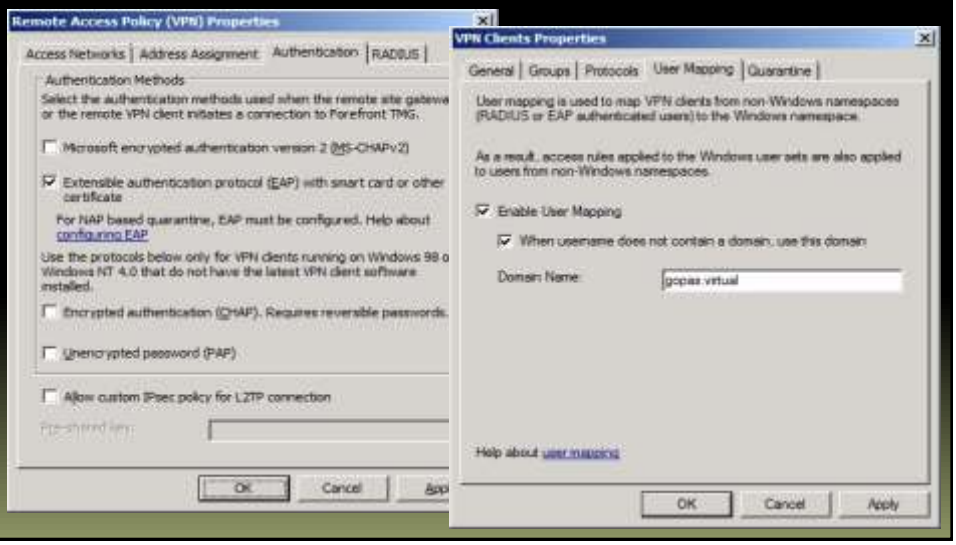
Password Authentication



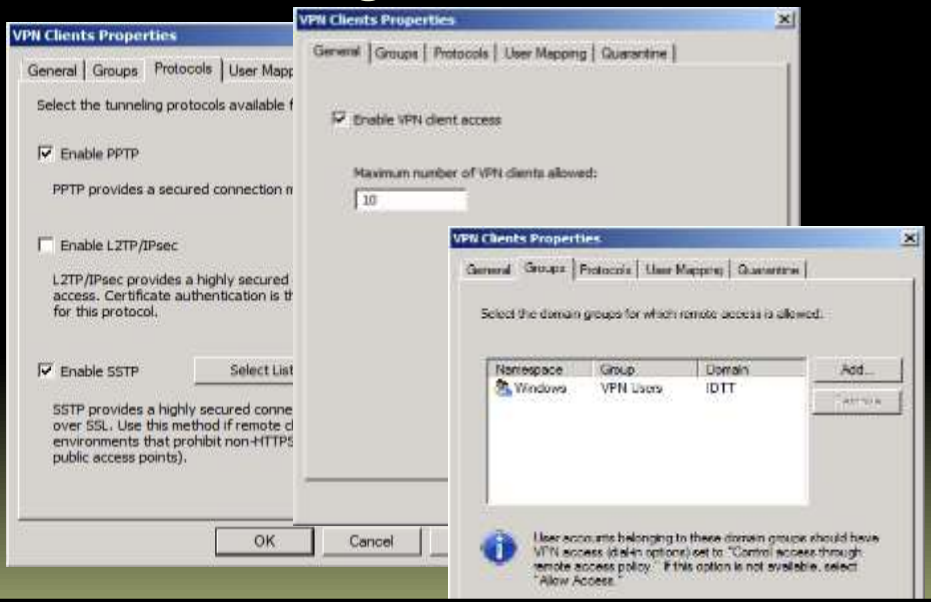
Client Certificate Authentication

- The most secure method
  - ideally stored on smart card
- The authenticated users belong to the RADIUS namespace
  - if you plan to use a user on a rule, it needs to be RADIUS user
- Or enable the user account mapping

Client Certificate Authentication



Other settings



Lab

- Add FW1 into RAS and IAS Servers group in Active Directory
  - restart the FW1 computer
- Enable VPN client access with password authentication
  - PPTP, VPN Users
- Create new Access Rule
  - Allow All outbound traffic from VPN Clients to Internal
  - Enable DCOM on the rule
- Move Seven1 computer to the Internet network
- Connect by using the VPN connection

Lab: Optional (if later doing NAP)

- On DC1 in Certification Authority console add User certificate template to be issued
- Reconfigure VPN to require EAP for authentication
- On Seven1 with VPN connected start certmgr.msc and Request new certificate based on the User template
- Reconfigure client and connect the VPN by using the client certificate

Threat Management Gateway 2010

SECURE SOCKET TUNNELING PROTOCOL

SSTP

- Clients starting with Windows Vista
- The best passing internet (just TCP 443)

SSTP Web Listener

- Requires Web Listener
- Will not authenticate users
  - the authentication settings do not apply
  - cannot be set to Require all users to authenticate
- SSL Certificate
  - the name must be that one used by the clients
  - CRL is always checked!

Lab

- Ensure that you have the following publishing rules for CRL
  - Web Listener
    - HTTP 80 on 81.0.0.178
  - Publishing rule
    - Public Name: ca.gopas.cz
    - Paths: /CertEnroll/*
    - To: dc1.gopas.virtual
    - Bridging: HTTP 80
    - Authentication Delegation: no delegation
- Confirm from the Seven1 client that the CRL is accessible from outside

Lab

- Ensure you the following web listener
  - HTTP 443 on 81.0.0.179
  - Certificate: *.gopas.cz
- Modify VPN settings to require SSTP using the web listener
- Confirm Seven1 can connect from the Internet

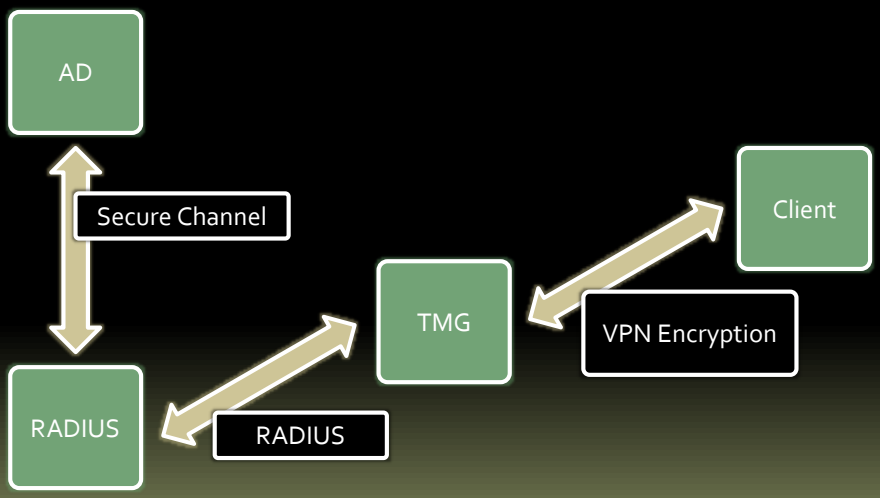
Threat Management Gateway 2010

RADIUS

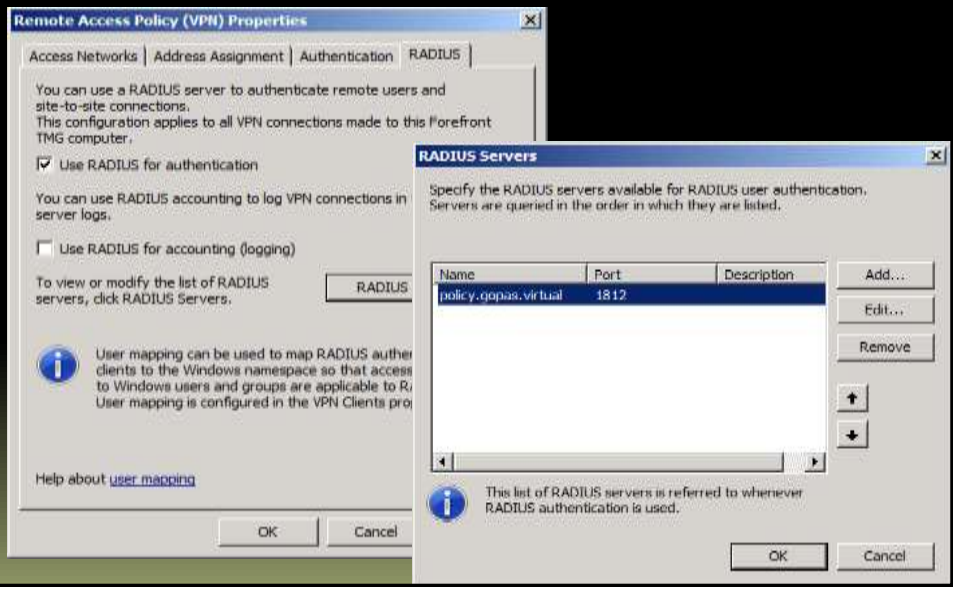
RADIUS Authentication

- Standard authentication server
  - UDP 1812
  - Internet Authentication Service (IAS)
  - Network Policy Server (NPS)
- Users not authenticated by TMG itself
- TMG needn't to be domain member
- Cannot use Windows user groups in firewall rules

Credentials Validation



RADIUS in TMG



Lab

- On POLICY enroll GOPAS Domain Server computer certificate
  - mmc
  - Add snap-in
  - Certificates – Local Computers
  - Request new certificate
  - GOPAS Domain Server
- Verify the certificate contains policy.gopas.virtual subject name with Server Authentication EKU

Lab

- On FW1 reconfigure VPN to authenticate users with RADIUS authentication
  - RADIUS server: POLICY
- On POLICY server configure FW1 as RADIUS client
- On POLICY server create Network Policy for VPN connections authenticated by EAP with Smart card or other certificate
  - or just password if you do not plan to do the NAP lab
- Test the VPN connectivity

Threat Management Gateway 2010

NETWORK ACCESS PROTECTION

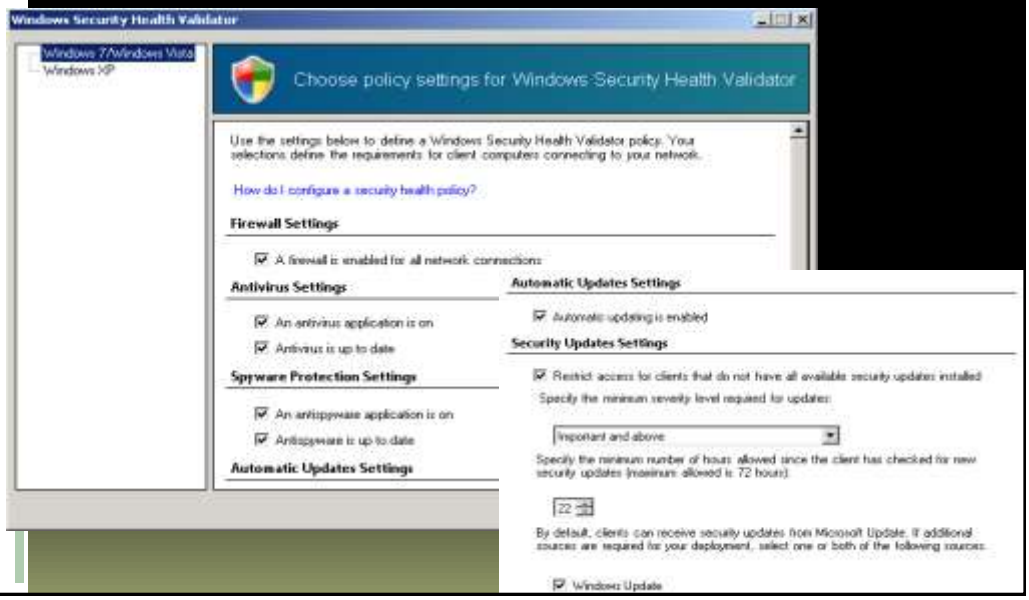
NAP

- Validates client health after actually connecting to the VPN server
  - client validates itself
  - not a security, just health test for not-infected clients
- Requires remote NPS server (RADIUS)
  - requires EAP authentication
- Allows for automatic remediation of the client settings
- Requires at least Windows XP SP3 client

Default Health Validator

- Is firewall enabled?
- Is antivirus/antispyware installed/enabled/up-to-date?
- Was the computer updated completely (to some severity) during several past days?

Default Health Validator



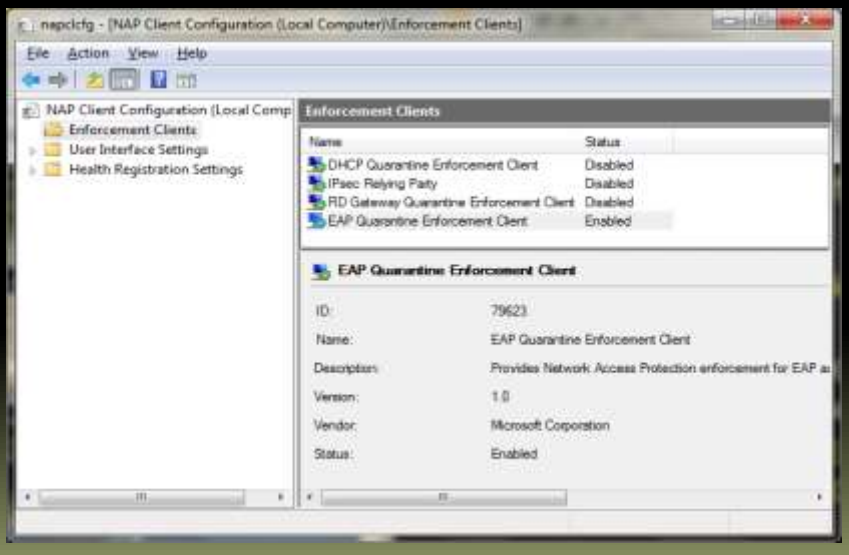
NAP in TMG

- Client connects to VPN and authenticates
- Client put into Quarantined VPN Clients network element
- Removed after successfully validates its health with NPS server

Client Configuration

- Enable and start Network Access Protection Agent service
- Ensure Security Center (XP, Vista) or Action Center (Windows 7) is enabled and running
- Enable EAP Quarantine Enforcement Client by using NAPCLCFG.MSC

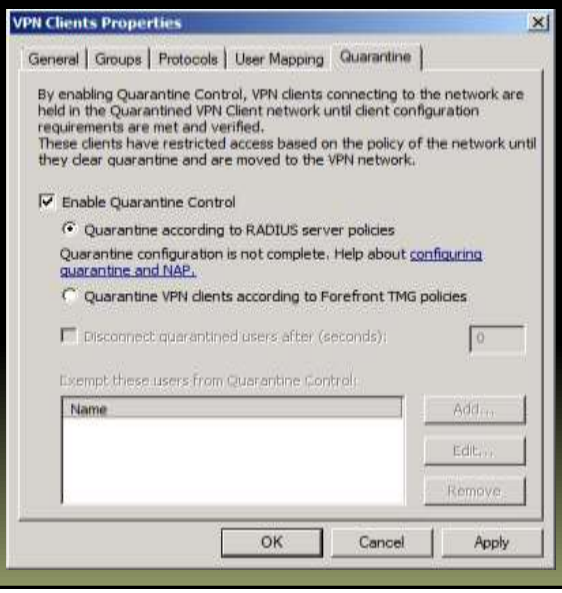
Client Configuration



TMG Configuration

- Manual reconfiguration of local NPS is not supported
- Remote NPS must be used instead
- TMG must quarantine the clients according to the NPS settings
  - client not removed until NPS leverages the quarantine

TMG Configuration



NPS Configuration

- Configure Health Validators
- Configure Network Access policy to require the health validation

Lab: Optional

- Reconfigure the NPS Network Policy and Health Validator to require Windows Firewall to be enabled on VPN clinets
- Reconfigure Seven1 client to have the NAP Enforcement Client enabled with EAP
- Test VPN connection with Windows Firewall disabled/enabled

Threat Management Gateway 2010

SITE-TO-SITE VPN

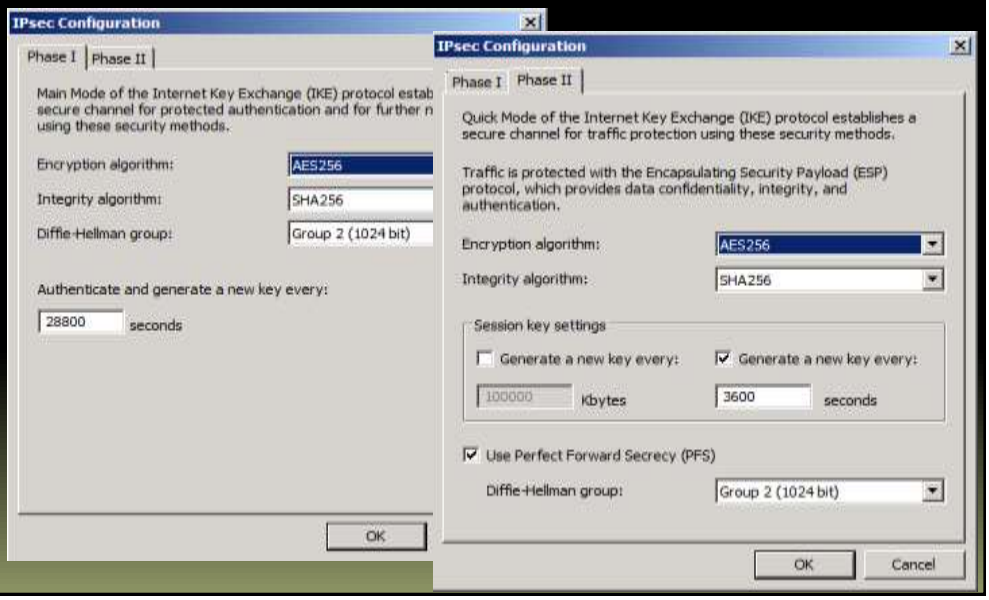
Protocol Selection

- PPTP, L2TP
  - requires user account to be used
  - PPTP insecure
- IPSec
  - standard method
  - compatible with various hardware devices

Default IPSec Parameters

- Usually must be adjusted
  - especially PFS
- Incompatible even with ISA 2006
  - uses AES/SHA-2

Default IPSec Parameters



Lab: Optional

- Configure IPSec tunnel between London office and the Prague central network
- You must test the connection from another computer (Seven1) placed in the London network
  - there wouldn't be a rule enabling FW2 traffic to Prague automatically

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

THANK YOU