www.crysys.hu

Network Security (BMEVIHIMB00)

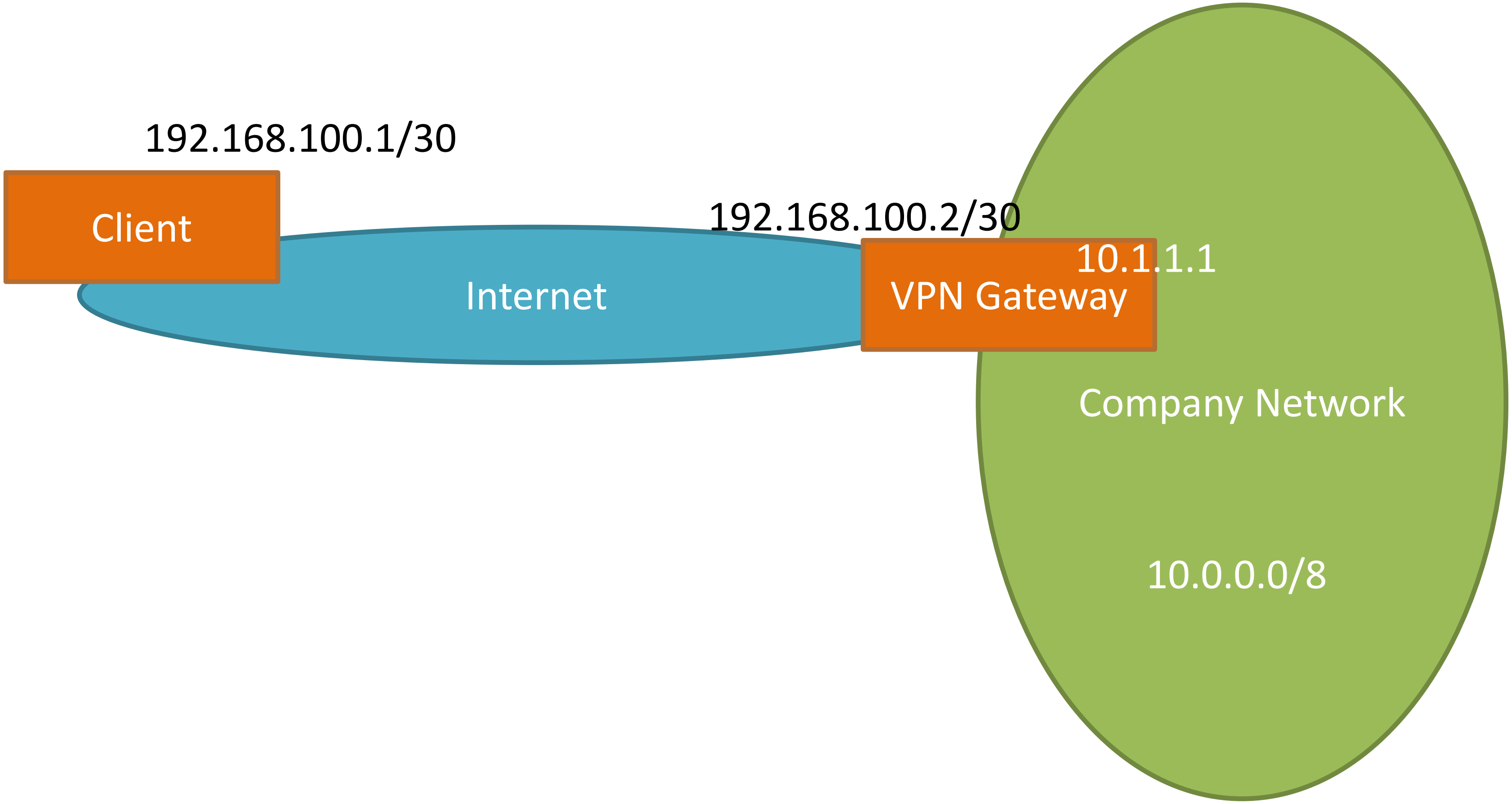
Practical Session: Virtual Private Networks

Gergő Ládi
Laboratory of Cryptography and System Security
Department of Networked Systems and Services
Gergo.Ladi@CrySyS.hu

Outline

- VPN with Windows Server
  - Setting up RRAS
  - Setting up clients
- IPSec with Windows
- OpenVPN
  - Setting up a server
  - Setting up a client

Network Topology



VPN WITH WINDOWS SERVER

VPN with Windows Server

- Virtual hardware
  - Client: 1 vNIC, internal network "Internet"
  - Server
    - 1 vNIC, internal network "Internet"
    - 1 vNIC, internal network "Company"

- Network addresses
  - Client: 192.168.100.1/30
  - Server
    - 192.168.100.2/30 (Internet)
    - 10.1.1.1/8 (Company)

VPN with Windows Server

- Testing the connection
  - Add a firewall rule to allow pinging the server from the client
  - Try pinging now… should work
- Install Wireshark on the client
- Setting up a web server in the company network (Server)
  - Open and edit lighttpd.conf on the server (lighttpd\conf\lighttpd.conf)
  - Find #server.bind
    - Remove #
    - Set bind address to 10.1.1.1
  - Start lighttpd

VPN with Windows Server

- Installing Routing and Remote Access (Server)
  - *Server Manager*, *Add Roles and Features*
  - Select *Remote Access*
  - Install *VPN* and *Routing* functionality

- Configuring RRAS (Server)
  - *Server Manager*, *Tools*, *Routing and Remote Access*
  - *Configure and Enable …*
  - Select *VPN and NAT*
    - » If it complains about not having 2 NICs, select *Custom*, then select *VPN* and *NAT*
  - Start the service

VPN with Windows Server

- Adding a static hosts entry (Client)
  - *notepad C:\Windows\System32\drivers\etc\hosts*
  - Add "192.168.100.2 vpn.gyakorlat.local" (without the quotes)

- Setting up a VPN connection (Client)
  - *Network and Sharing Center, Set up a new connection or network*
  - *Connect to a workplace, Use my Internet connection (VPN)*
  - Enter *vpn.gyakorlat.local* for the name
  - Try to connect (Administrator/Admin1)…

VPN with Windows Server

- Allowing *Administrator* to connect to the VPN (Server)
  - *lusrmgr.msc*
  - *Users*, *Administrator*, *Properties*, *Dial-In*
  - *Allow access*

- Connecting to the VPN (Client)
  - The connection should succeed
  - Ping 10.1.1.1… failed… why?
  - Check your IP address, it's 169.254.x.y… why?

VPN with Windows Server

- Setting up RRAS to assign addresses to VPN clients (Server)
  - RRAS, Properties, IPv4
  - Set it to assign IP addresses from a subnet of the 10.0.0.0/8 pool
  - Restart RRAS

- Connecting to the VPN (Client)
  - The connection should succeed
  - What IP did you get?
  - Ping 10.1.1.1 – should work
  - Open 10.1.1.1 in the browser – you should see the "company webpage"

VPN with Windows Server

- Inspecting VPN traffic with Wireshark (Client)
  - Start capturing on the "internet" interface
  - Refresh the company page in the browser
  - Which method was used to connect?

- Setting the VPN connection to use SSTP (Client)
  - *Network and Sharing Center*, select the VPN connection
  - *Properties*, *Security*, *Type of VPN*
  - Try to connect now…

VPN with Windows Server

- Installing an X.509 certificate on the VPN server (Server)
  - Download the .pfx file from the subject's website
  - Import it to the *Local Machine*'s *Personal* certificate store
  - The password is: *asd*

- Setting the VPN server to use the new certificate (Server)
  - Open the Routing and Remote Access management tool
  - Select the server, right click it
  - On the *Security* tab, under *SSL Certificate Binding*, select the newly installed certificate
  - Restart the service

VPN with Windows Server

- Connecting to the SSTP VPN (Client)
  - Try connecting now…
  - We have to install the certificate on the client as well, using the same .pfx
  - Install the certificate to the *Local Machine*'s *Trusted Root Certificate Authorities* container
    - Of course, we don't need the server's private key on the client (and you should never disclose the server's private key to clients), but for the purposes of the demo, we don't care… it's faster this way
  - Try connecting now…
  - Inspect traffic in Wireshark

VPN with Windows Server

- Connecting using L2TP (Client)
  - *Network and Sharing Center*, select the VPN connection
  - *Properties*, *Security*, *Type of VPN*
  - Try to connect now…
  - Needs a machine cert… we don't have one…
  - Under Advanced Settings, set it to use a PSK instead of a certificate

- Setting the VPN server to use a PSK (Server)
  - Open the Routing and Remote Access management tool
  - Select the server, right click it
  - On the *Security* tab, tick *Allow custom IPsec policy for L2TP/IKEv2 connection*
  - Enter the same PSK as chosen above
  - Restart the service

VPN with Windows Server

- Connecting using L2TP (Client)
  - Start capturing in Wireshark
  - Try connecting now…
  - What version of IKE is being used?

- Observing Security Associations (Client)
  - Open *Windows Firewall* (wf.msc)
  - Under *Monitoring*, select *Security Associations*
  - What can be seen under Main Mode and Quick Mode?

VPN with Windows Server

- Connecting using IKEv2 (Client)
  - Set the client to use IKEv2 instead of L2TP
  - Try connecting now…
  - Unfortunately, it doesn't work with our cert

  - Alternative: observe the ISAKMP messages in Wireshark (IKEv2.pcap)

IPSEC WITH WINDOWS

IPSec with Windows

- Creating the Connection Security Rule (Client)
  - Open Windows Firewall
  - Right-click *Connection Security Rules*, then *New Rule*…
  - Rule type: custom
  - Endpoints: 192.168.100.1 and 192.168.100.2
  - Require authentication for inbound and outbound connections
  - Authentication method: Advanced
    - *Customize*…
    - *Add, Preshared key (not recommended)*
    - Choose a PSK
  - Next, next, finish

- Creating the Connection Security Rule (Server)
  - Same steps, except the endpoints should be in reverse order

IPSec with Windows

- Observing traffic (Client)
  - Start pinging the server
  - Start a capture in Wireshark
  - Notice anything strange?

- Observing Security Associations (Client)
  - What's different here (compared to L2TP and IKEv2)?

OPENVPN

OpenVPN

- Note: key generation is typically done on a dedicated machine (the VPN CA). For the purposes of this demo and to save time, we'll do everything on one machine, then clone the machine.

- Key generation

```
– cd /usr/share/easy-rsa
– source vars
– ./clean-all
– ./build-ca # Produces ca.key and ca.crt
– ./build-key-server server # Prod. server.key and .crt
– ./build-key client1 # Produces client1.key and .crt
– ./build-dh # Produces dh####.pem (here, ####==2048)
– openvpn --genkey --secret secret.key # Optional
```

OpenVPN

- Network configuration (`nano /etc/network/interfaces`)
  - Client

```
auto enp0s3
iface enp0s3 inet static
        address 192.168.100.1
        netmask 255.255.255.252
```

  - Server

```
auto enp0s3
iface enp0s3 inet static
        address 192.168.100.2
        netmask 255.255.255.252

auto enp0s8
iface enp0s8 inet static
        address 10.1.1.1
        netmask 255.0.0.0
```

OpenVPN

- Client configuration
  - nano /etc/openvpn/client.conf

```
client
tls-client
remote 192.168.100.2
dev tap
cipher AES-256-GCM
auth SHA512

ca ca.crt
cert client1.crt
key client1.key

# If a secret.key was generated for extra control channel encryption
# tls-crypt secret.key
```

  - Reboot/reload

OpenVPN

- Server configuration
  - `nano /etc/openvpn/server.conf`

```
server 172.16.0.0 255.255.0.0

dev tap
cipher AES-256-GCM
auth SHA512

cert server.crt
key server.key
ca ca.crt
dh dh2048.pem

push "route 10.0.0.0 255.0.0.0 172.16.0.1"
# If a secret.key was generated for extra control channel encryption
# tls-crypt secret.key
```

  - Reboot/reload

www.crysys.hu

Thank you for your attention!

Questions?

Gergő Ládi
Laboratory of Cryptography and System Security
Department of Networked Systems and Services
Gergo.Ladi@CrySyS.hu

MISCELLANEOUS

Control Questions

- What VPN protocols are available by default on Windows?
- Which Windows Server Role needs to be installed in order to host a VPN server with Windows?
- What is needed for SSTP to work?
- You have successfully connected to your VPN server, but you can't access anything. You check your connection, and see that your IP address is 169.254.123.213. What could be the reason?
- What version of IKE is used for these VPNs: L2TP, SSTP, IKEv2?
- What version of IKE is used for the built-in Connection Security rules?
- Which protocol is used for encapsulation in OpenVPN?
- In OpenVPN deployments, which of these have to be present on the OpenVPN server, and which on the client?
  - ca.crt, ca.key, server.key, server.crt, client.crt, client.key, dh####.pem
- You are attempting to connect to your company's VPN server, but you can't. Give at least 4 examples why this might be happening.

www.crysys.hu

Network Security (BMEVIHIMB00)

Practical Session: Virtual Private Networks

Gergő Ládi
Laboratory of Cryptography and System Security
Department of Networked Systems and Services
Gergo.Ladi@CrySyS.hu