TROOPERS

ERNW
providing security.

Security Assessment of Microsoft DirectAccess

A thesis for the completion of Master of Science in Communication and Media Engineering CME

By

Ali Hardudi

Supervised by

Prof. Dr. rer. nat. habil. **Dirk Westhoff**

M. Sc. **Enno Rey**

Agenda

- Introduction
  - Objective
  - A Quick Look into DirectAccess
- DirectAccess Lab
- Assessment
  - Scenarios and Attacker
  - IPv6 Attacks
  - TLS and IPSEC Default Configuration
- Conclusion

Introduction

Thesis Objective

- Thesis objective
  - Study the DirectAccess
  - Performing a security evaluation

DirectAccess Features

- ✓ Pure IPv6
- ✓ No user interaction
- ✓ Remote management and administration
- ✓ Bidirectional access
- ✓ Enhanced security features
- ✓ Working over IPv4 Internet infrastructure

DirectAccess Limitations

- Not all Windows OS's are supported
- The following options are not always possible:
  - End to End encryption
  - Force tunneling
- Performance degradation when IP-HTTPS tunneling is used
- Complex technology

Technologies and Protocols

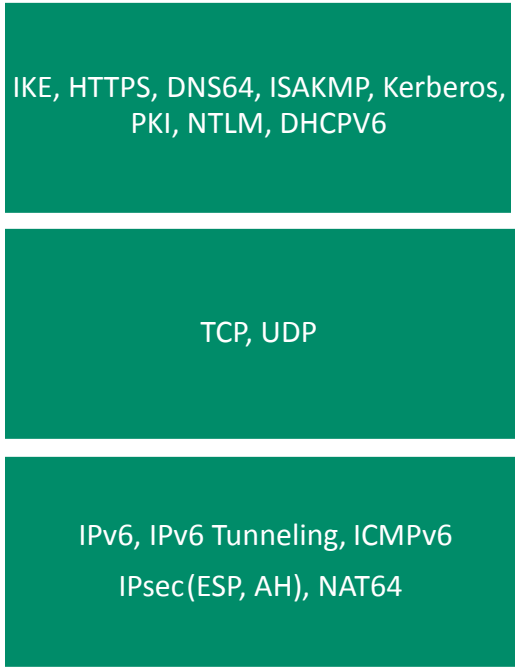


Figure 1 DirectAccess stack of main protocols

- Active Directory Domain Controller (AD DC).
- IPSEC
- Public Key Infrastructure (PKI)
- HTTPS server as Network Location Service (NLS)
- Name Resolution Policy Table (NRPT)
- IPv6 tunneling technologies
- NAT64/DNS64
- Others (e.g. Forefront Unified Access Gateway (UAG), Network Access Protection (NAP))

Figure 2 DirectAccess connection steps using IP-HTTPS

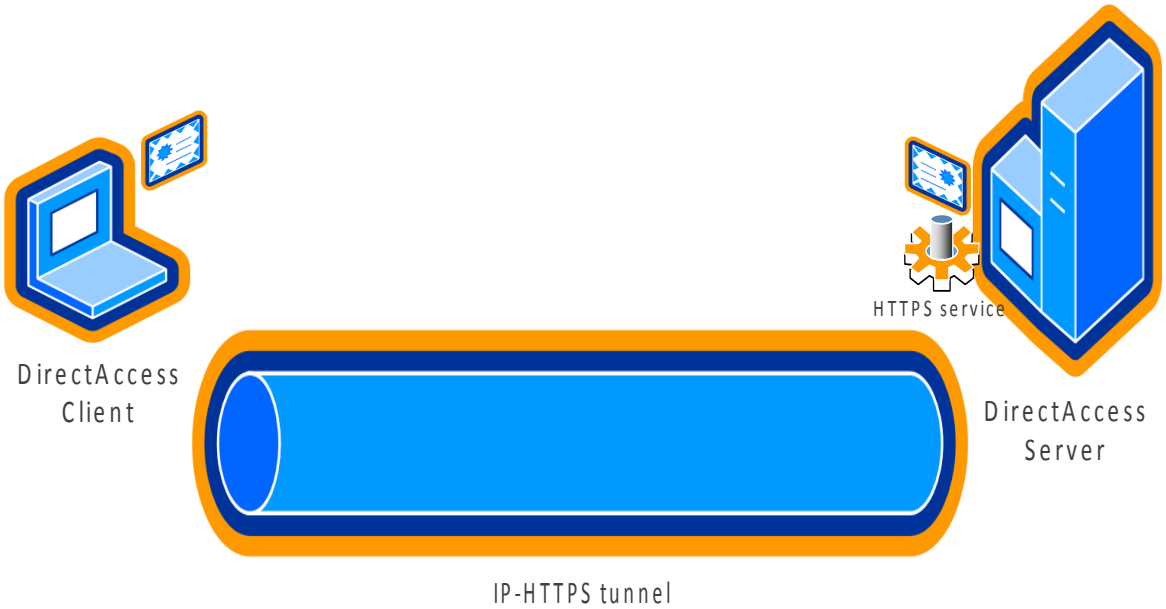


Figure 2 DirectAccess connection steps using IP-HTTPS

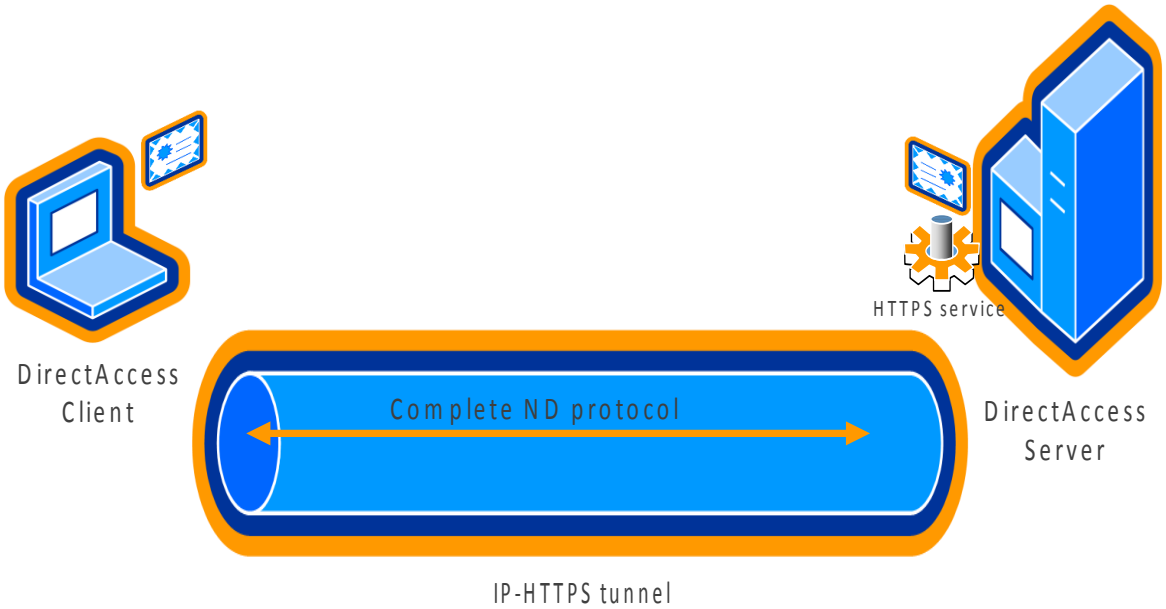


Figure 2 DirectAccess connection steps using IP-HTTPS

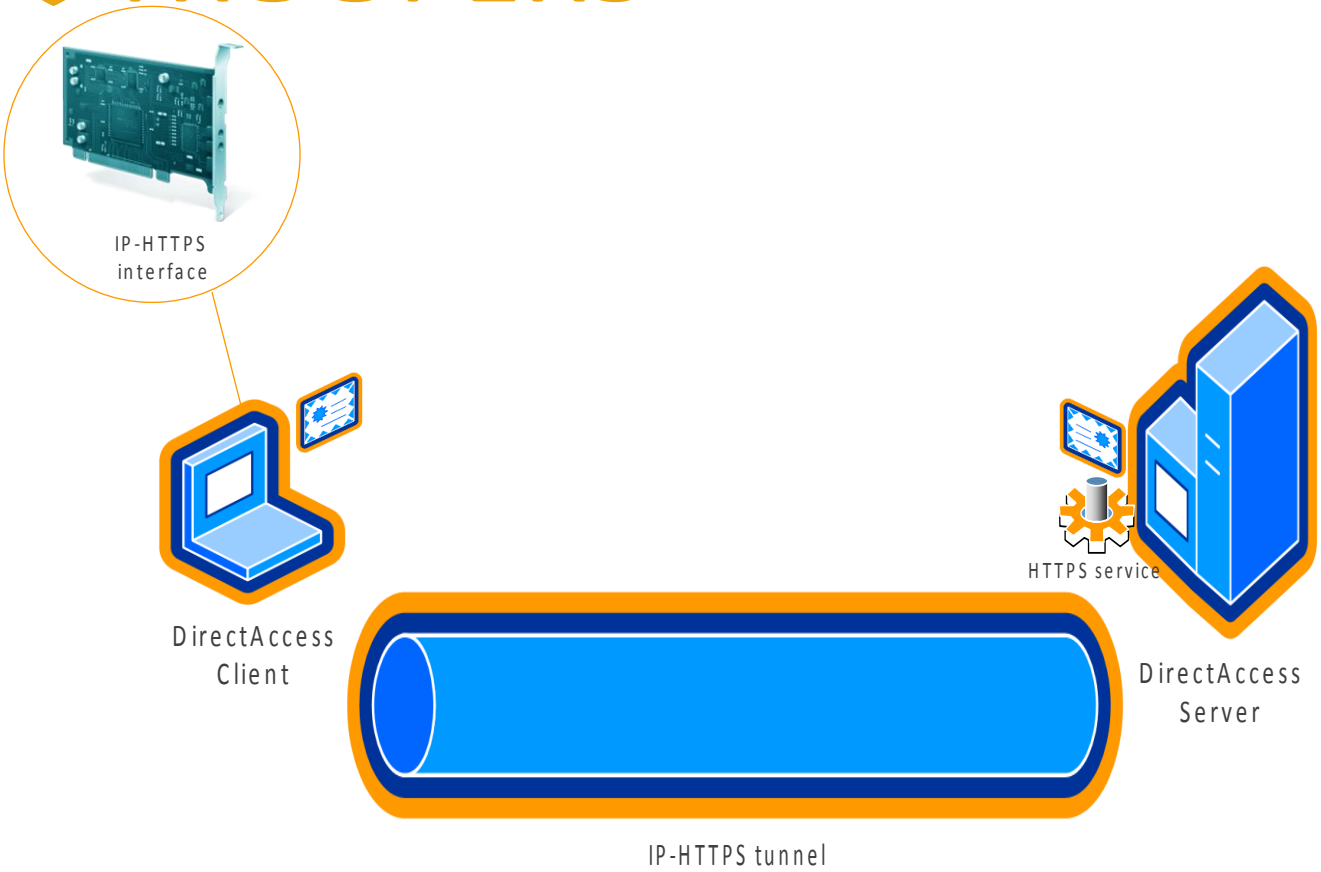


Figure 2 DirectAccess connection steps using IP-HTTPS

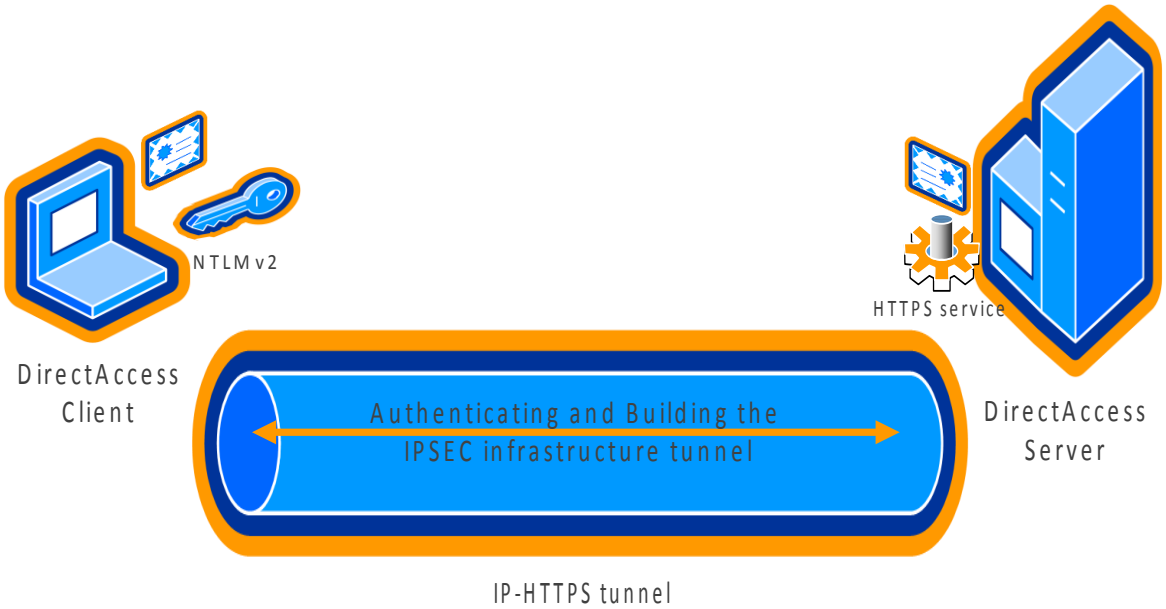


Figure 2 DirectAccess connection steps using IP-HTTPS

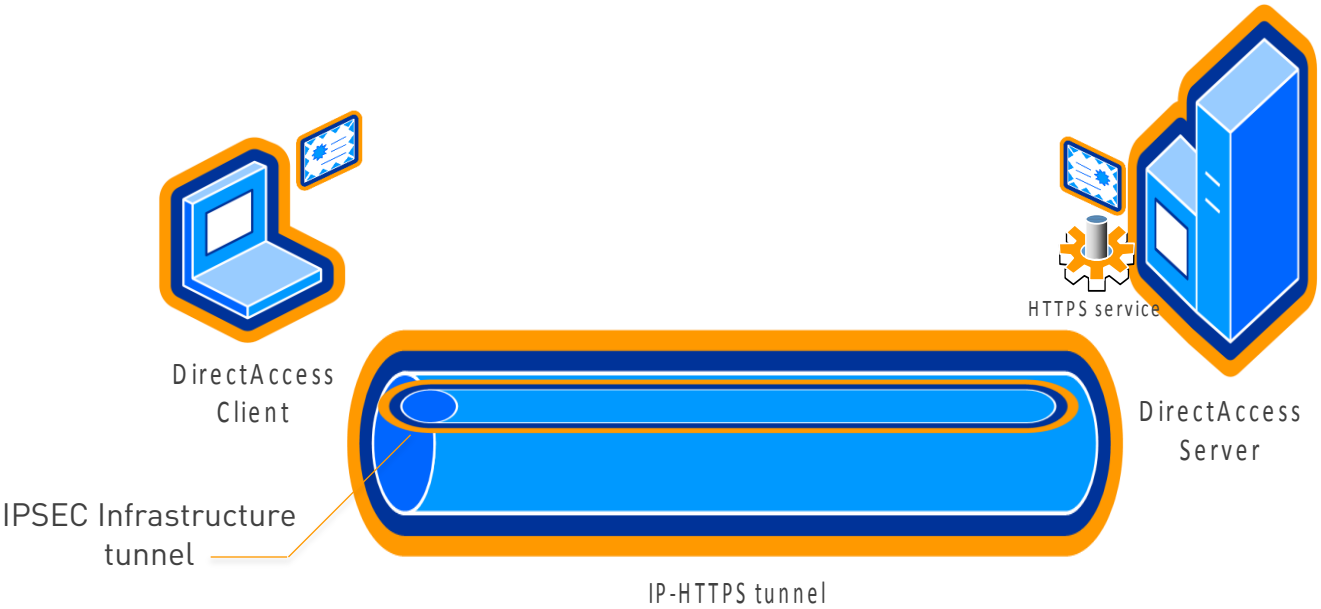


Figure 2 DirectAccess connection steps using IP-HTTPS

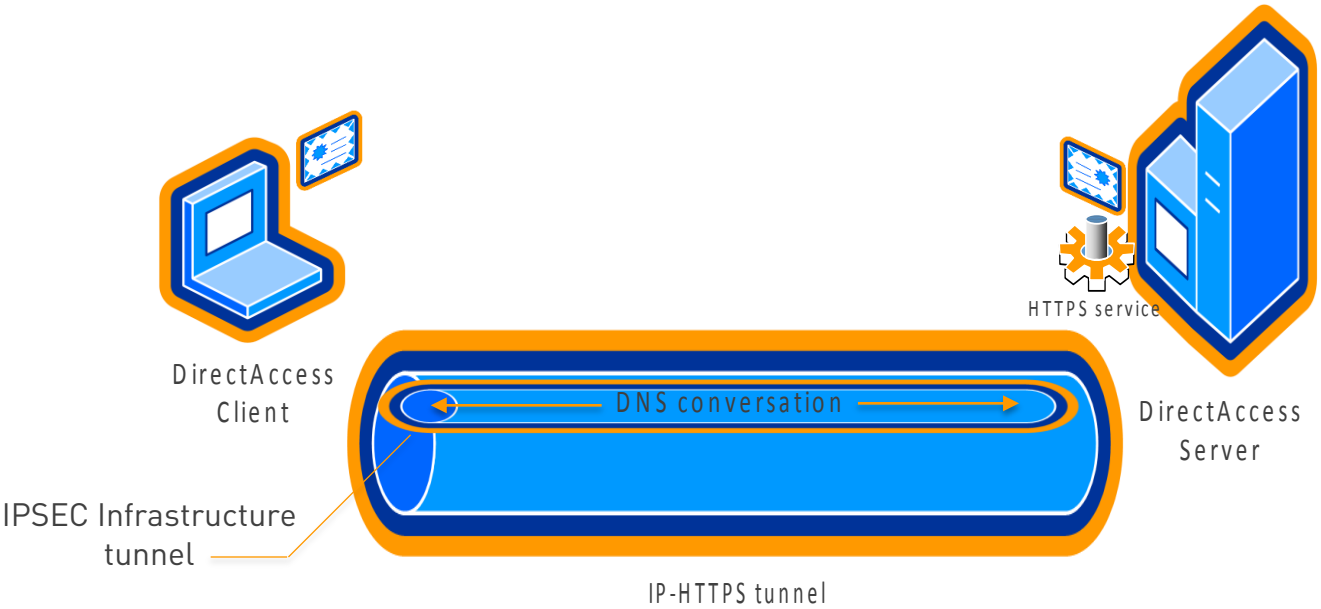


Figure 2 DirectAccess connection steps using IP-HTTPS

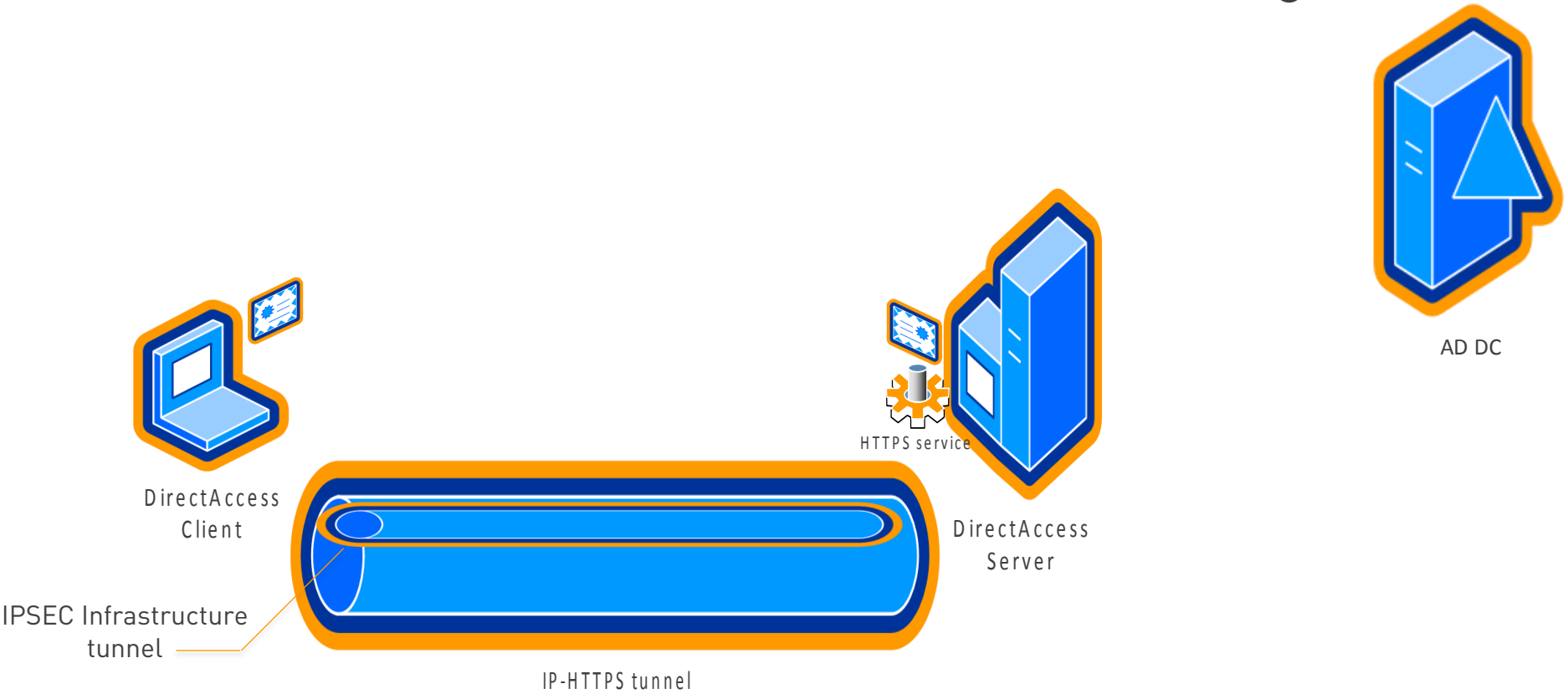


Figure 2 DirectAccess connection steps using IP-HTTPS

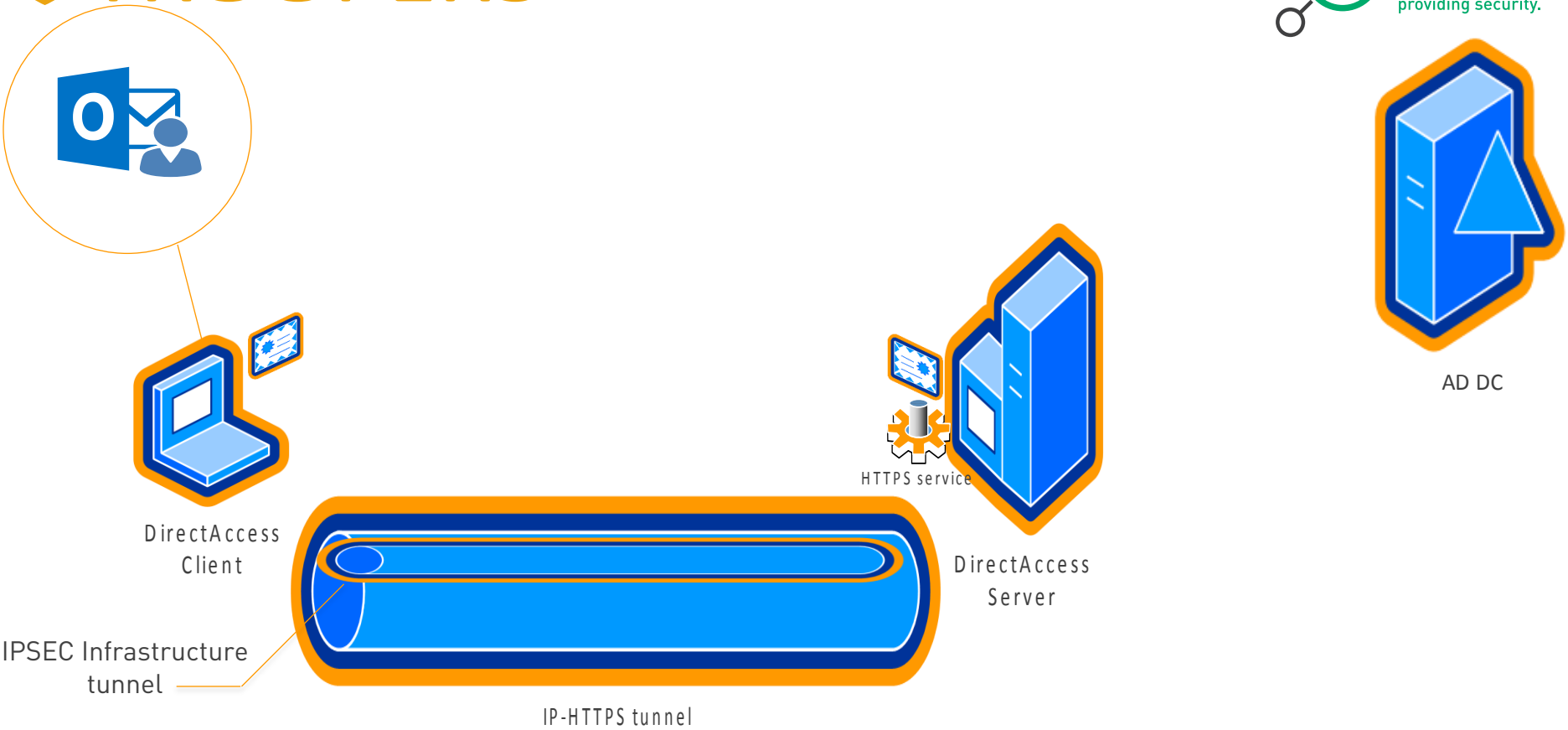


Figure 2 DirectAccess connection steps using IP-HTTPS

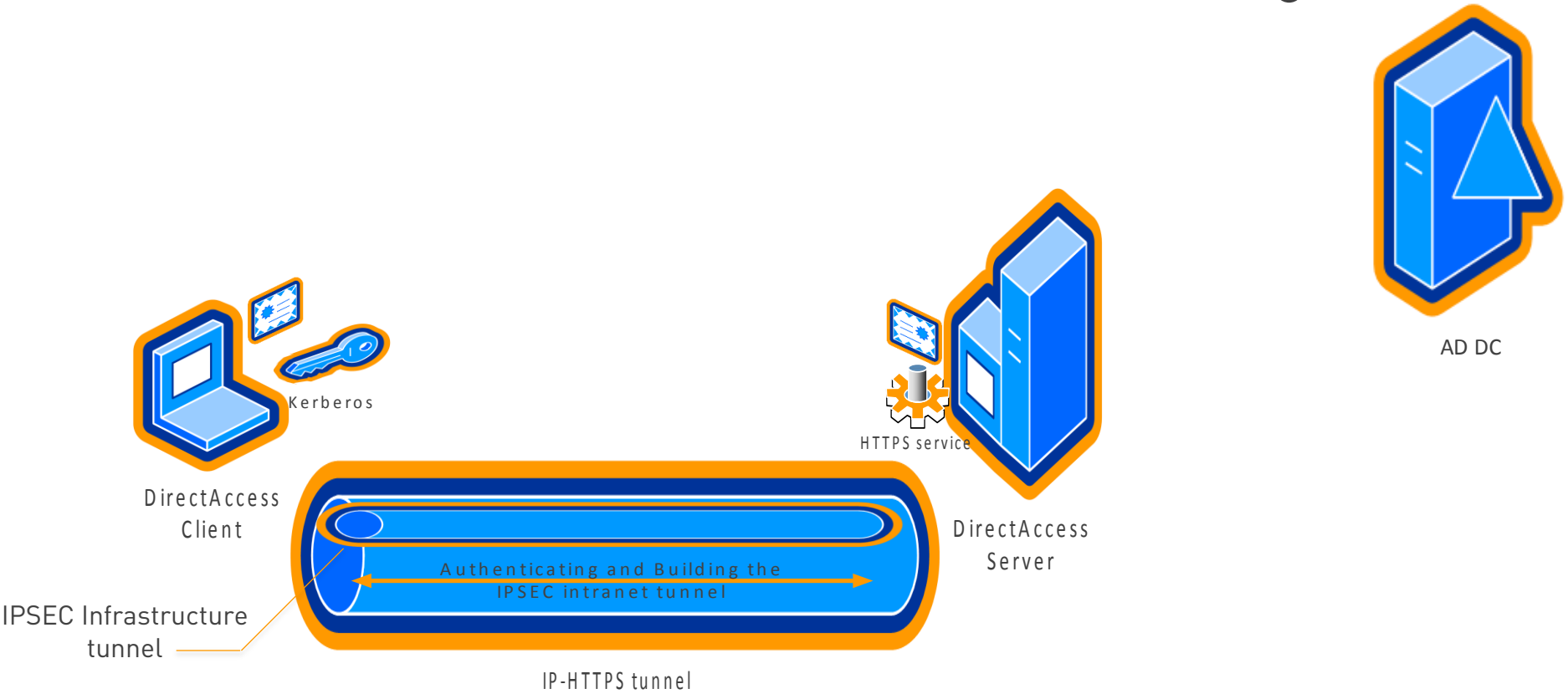


Figure 2 DirectAccess connection steps using IP-HTTPS

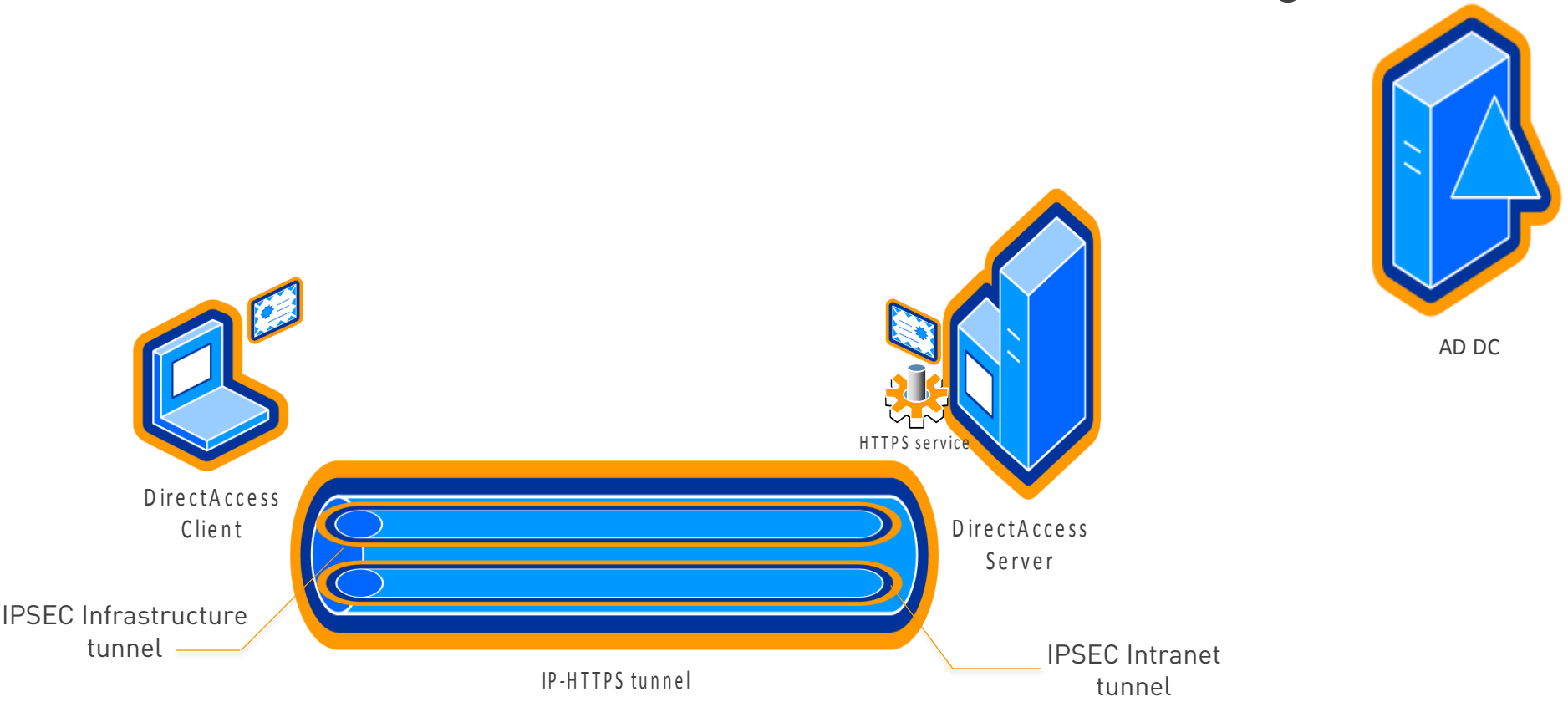


Figure 2 DirectAccess connection steps using IP-HTTPS

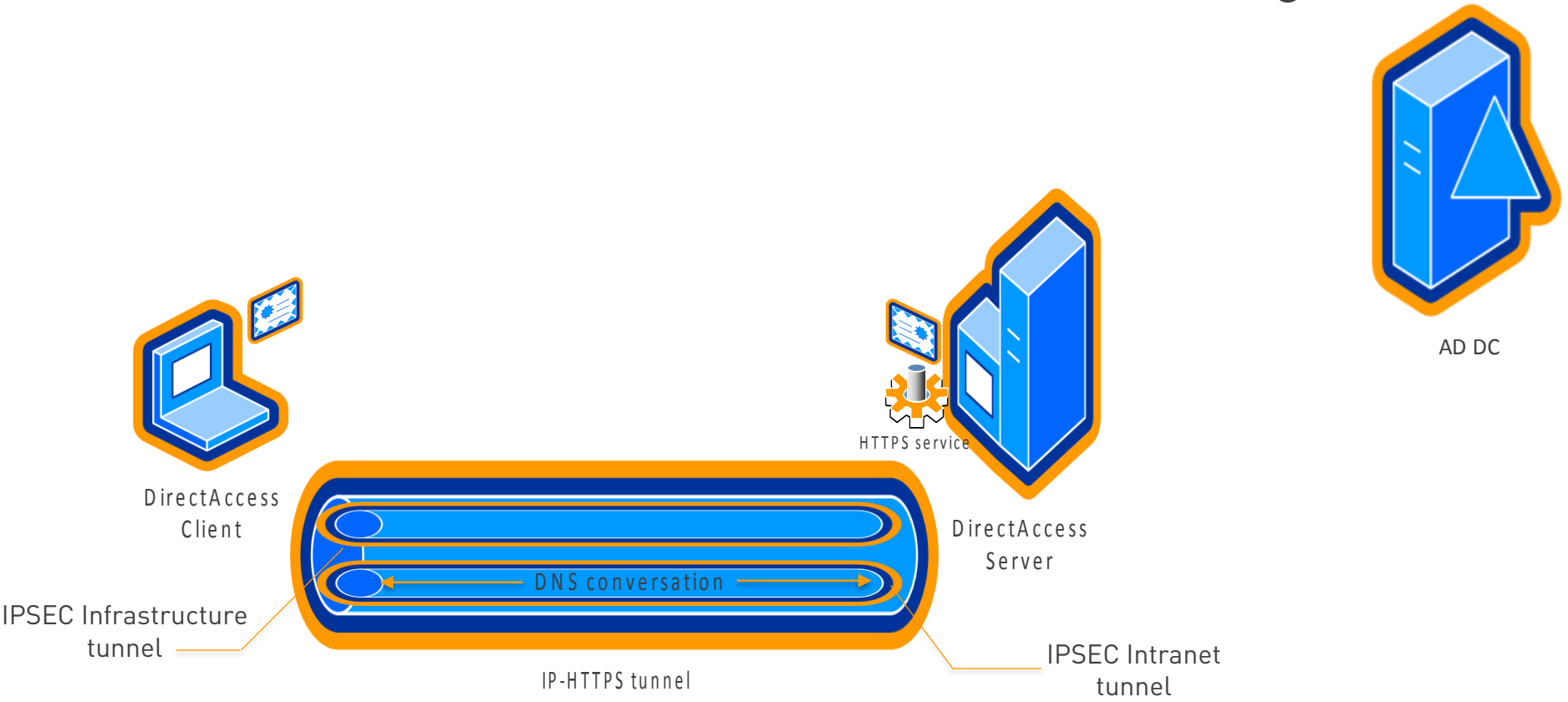


Figure 2 DirectAccess connection steps using IP-HTTPS

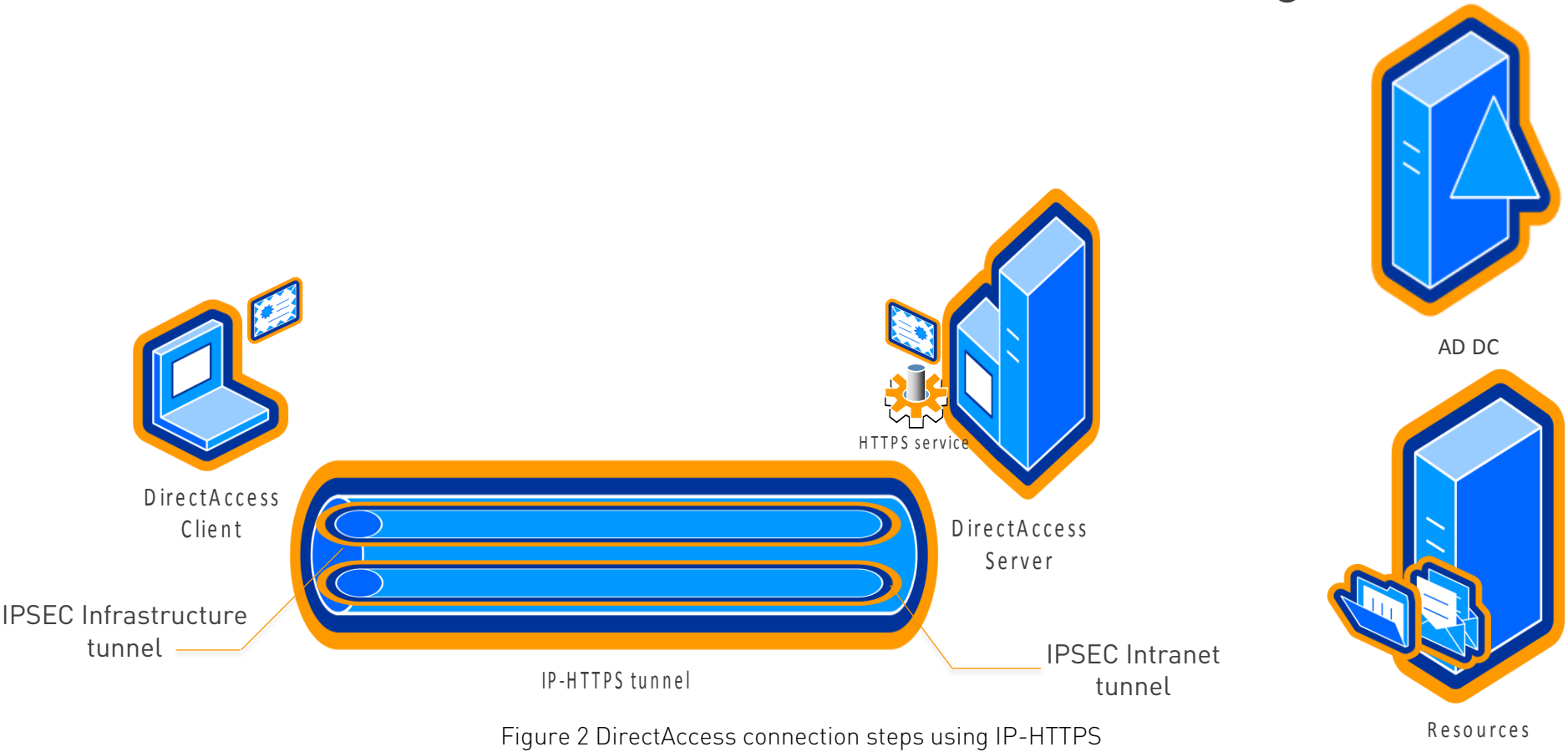


Figure 2 DirectAccess connection steps using IP-HTTPS

Lab Deployment

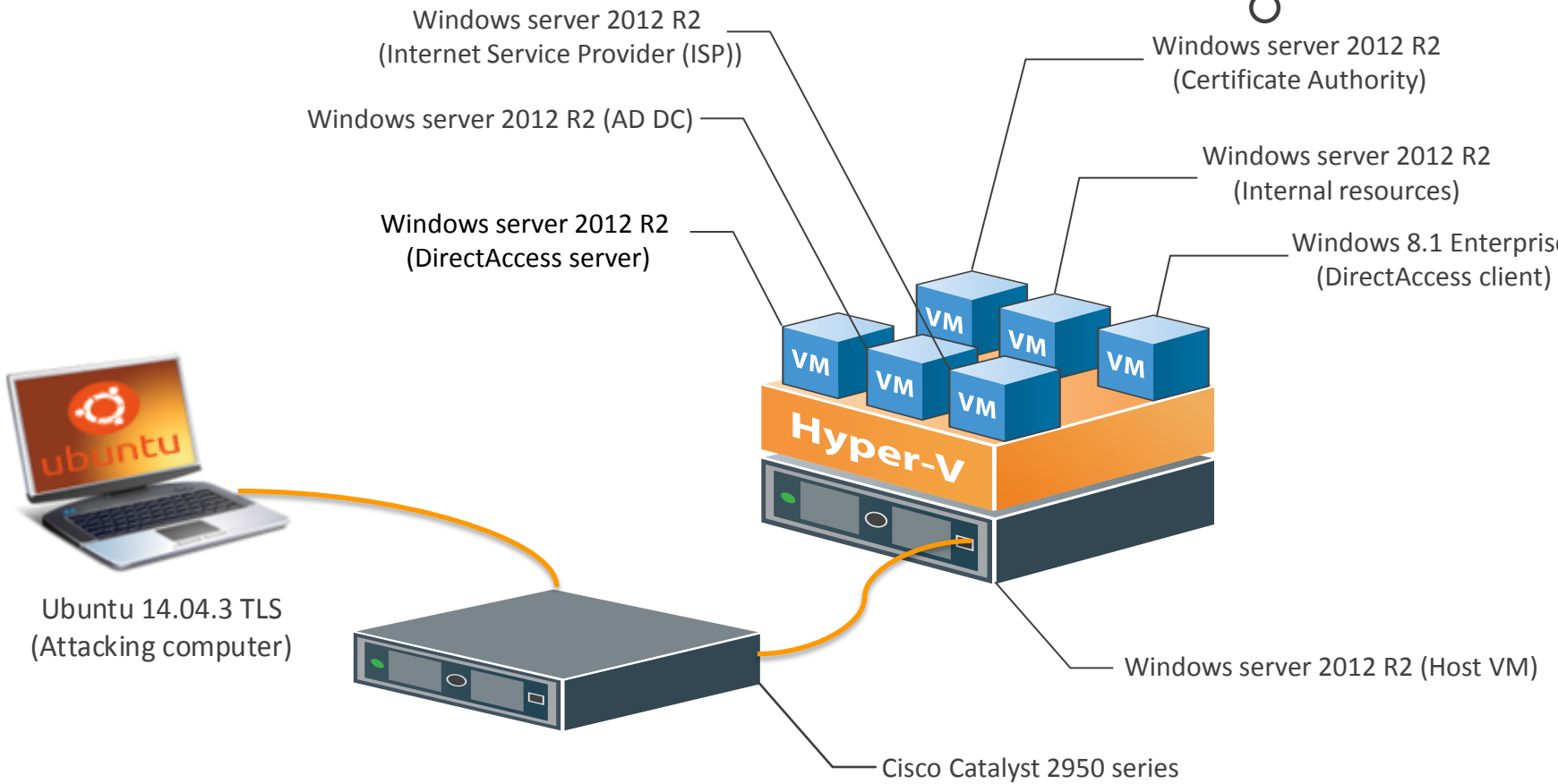


Figure 3 DirectAccess lab components

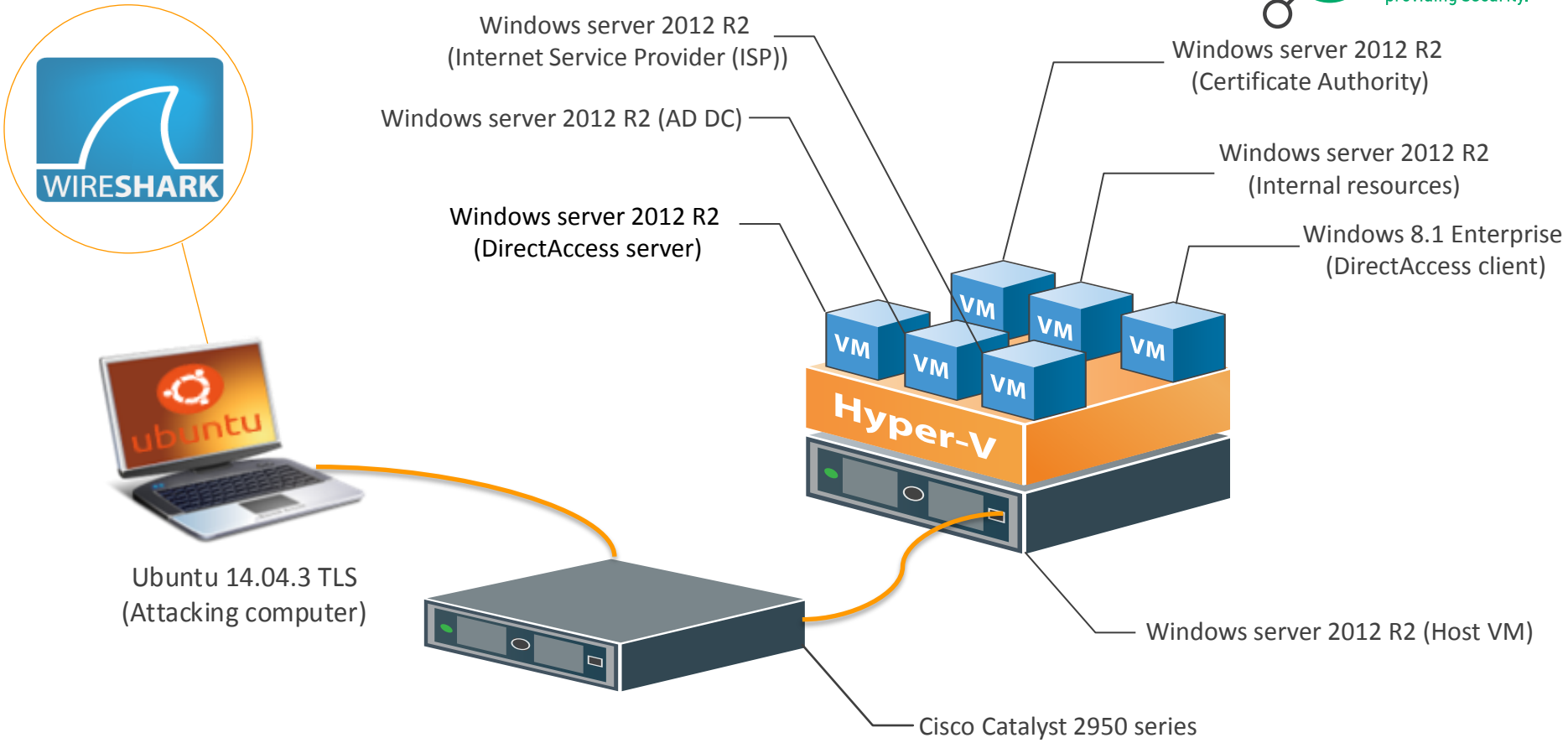
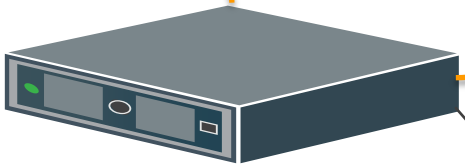
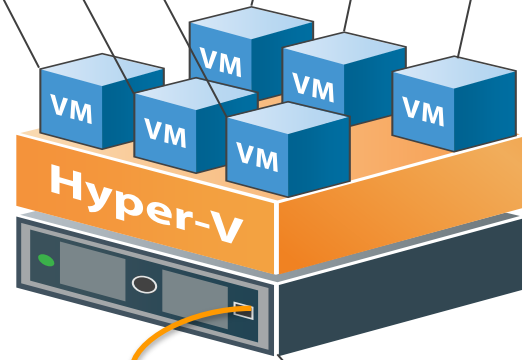


Figure 3 DirectAccess lab components

Ubuntu 14.04.3 TLS
(Attacking computer)



Cisco Catalyst 2950 series



Windows server 2012 R2 (Host VM)

Windows server 2012 R2
(Internet Service Provider (ISP))

Windows server 2012 R2 (AD DC)

Windows server 2012 R2
(DirectAccess server)

Windows server 2012 R2
(Certificate Authority)

Windows server 2012 R2
(Internal resources)

Windows 8.1 Enterprise
(DirectAccess client)

Figure 3 DirectAccess lab components

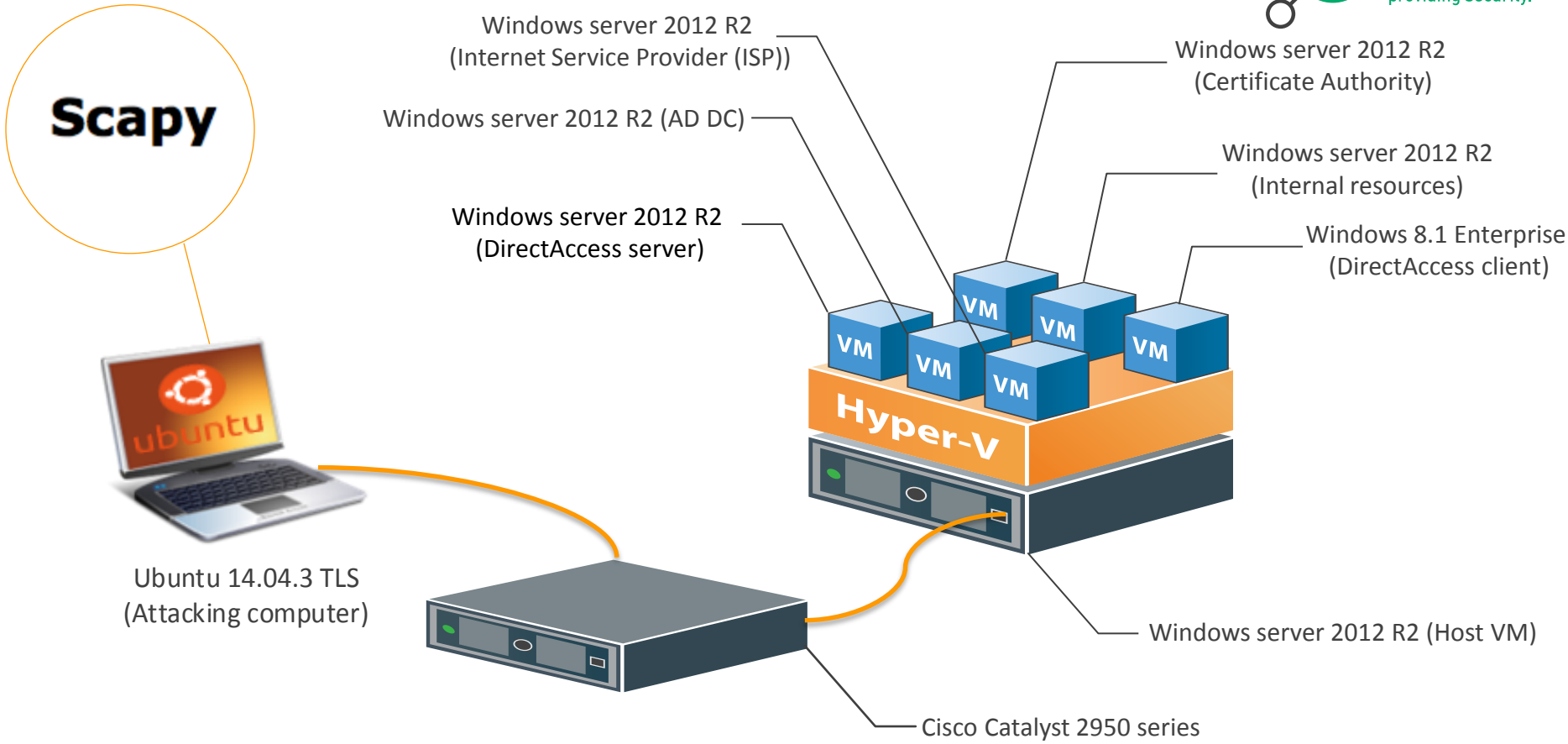


Figure 3 DirectAccess lab components

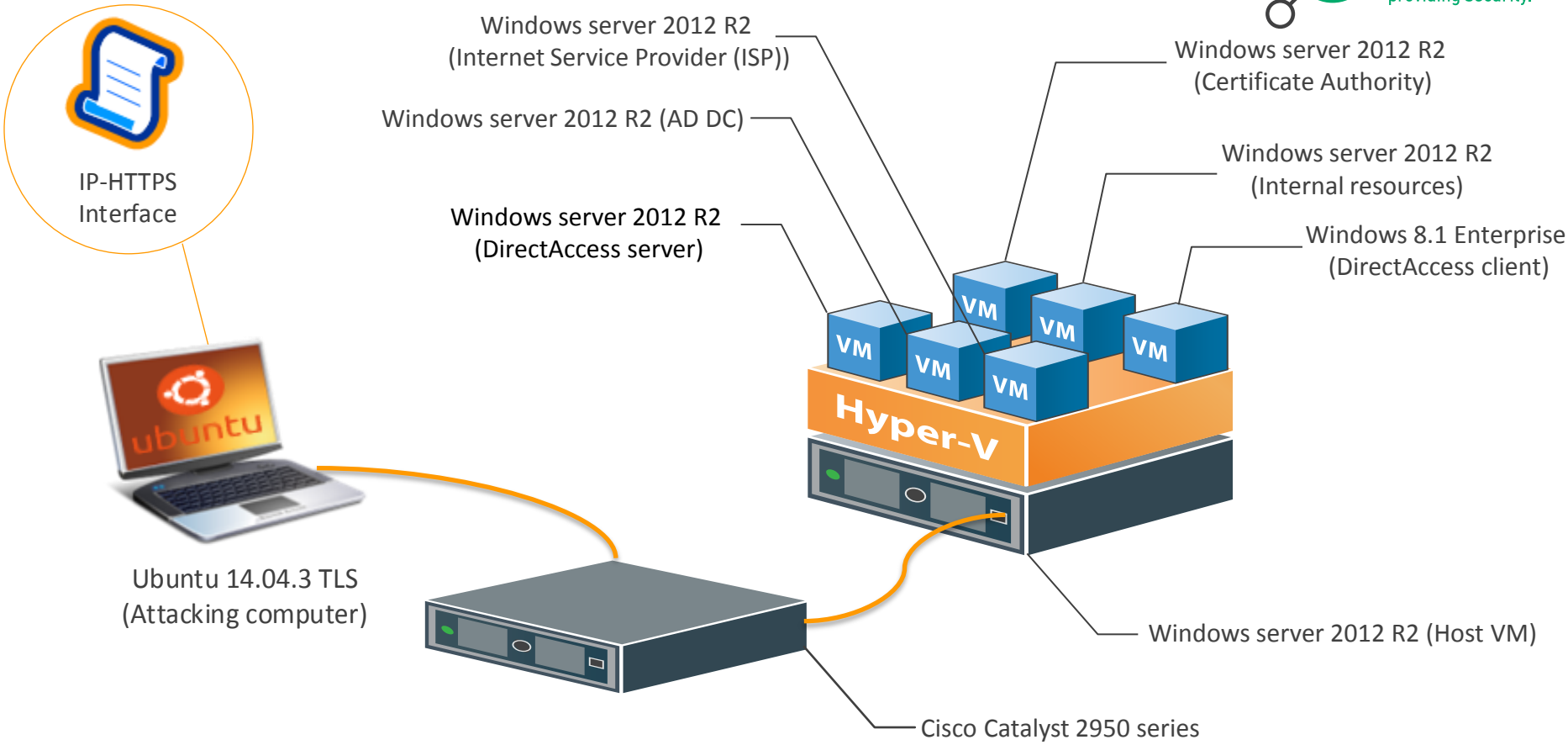


Figure 3 DirectAccess lab components

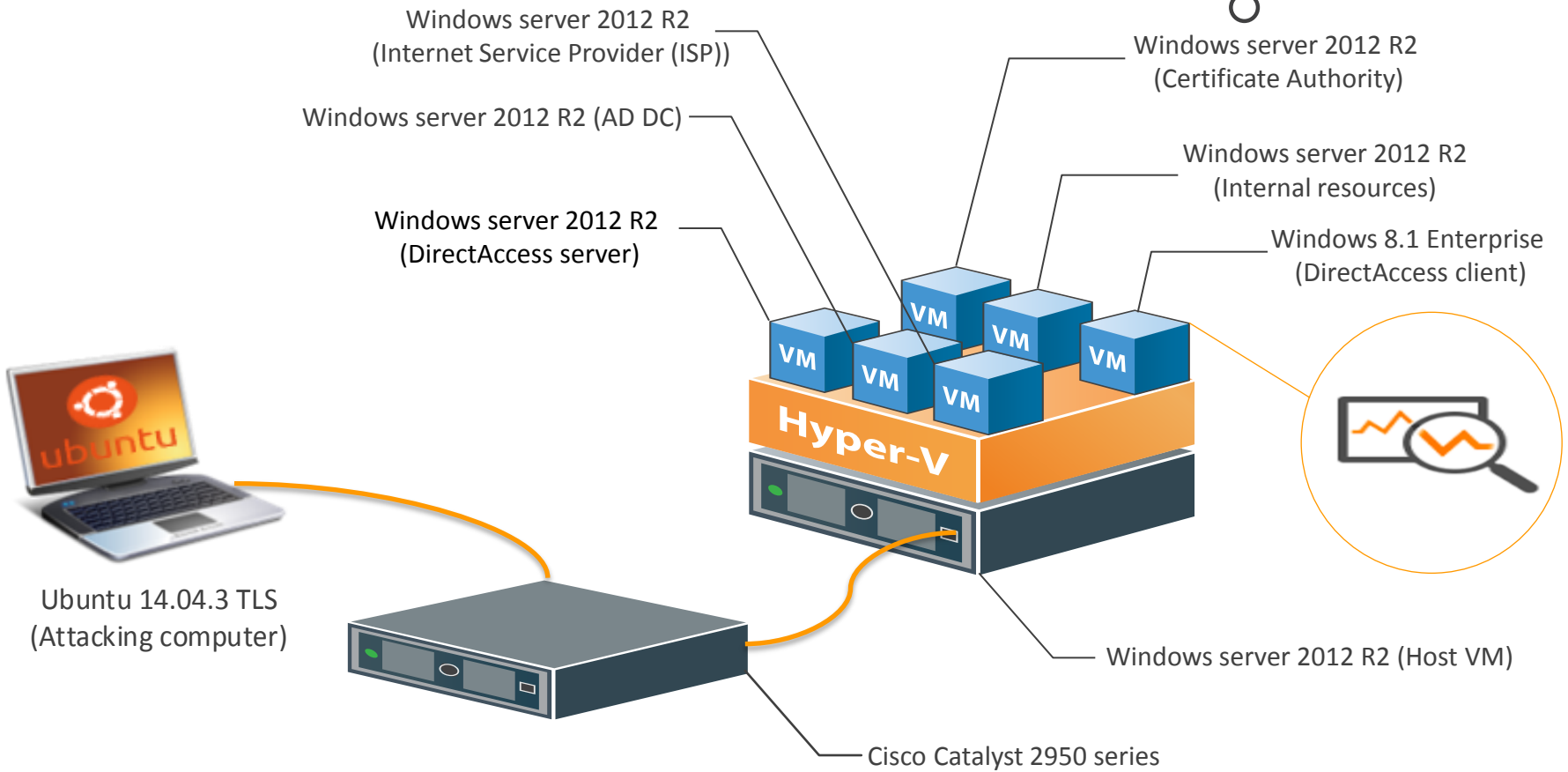


Figure 3 DirectAccess lab components

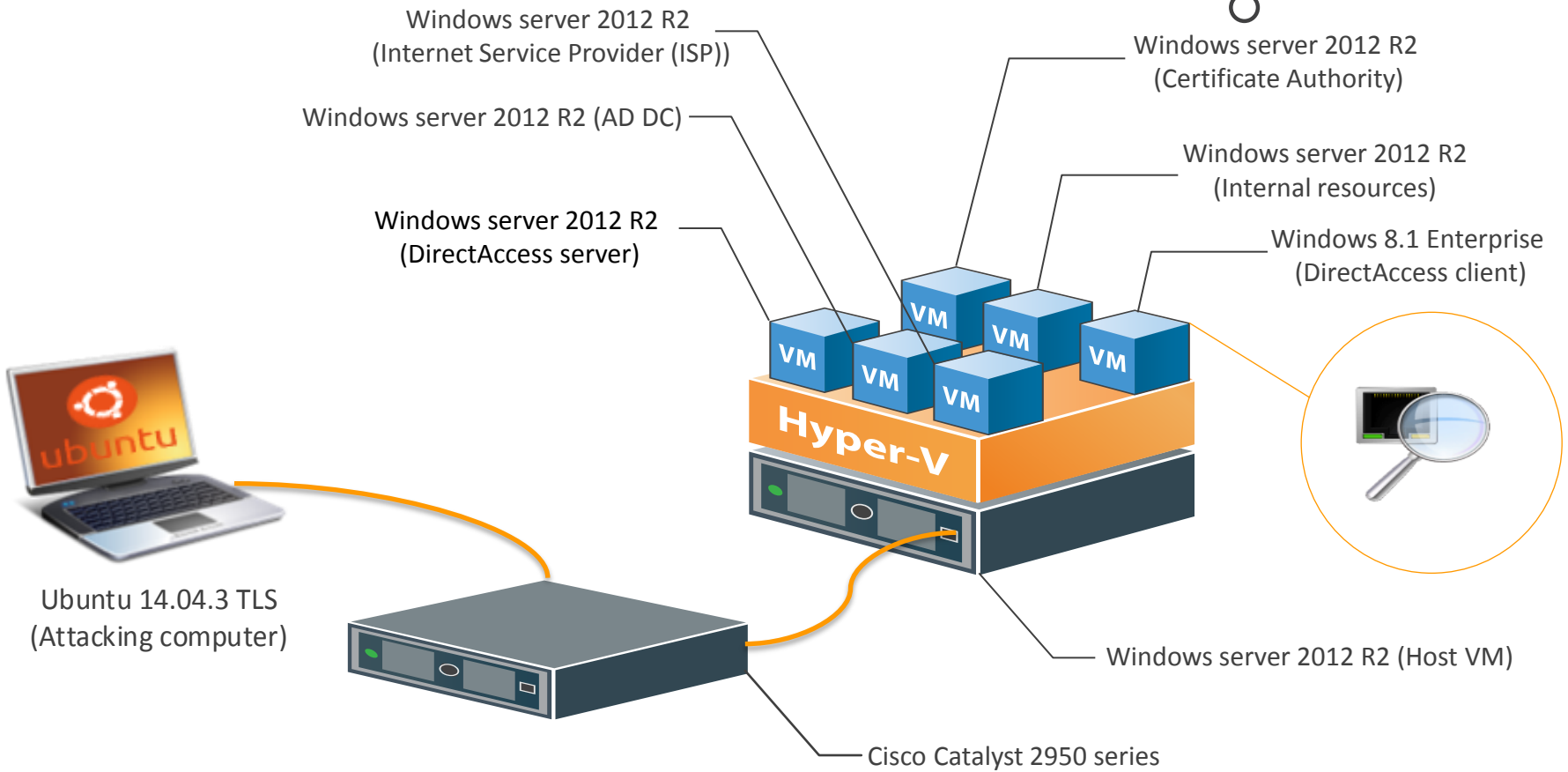


Figure 3 DirectAccess lab components

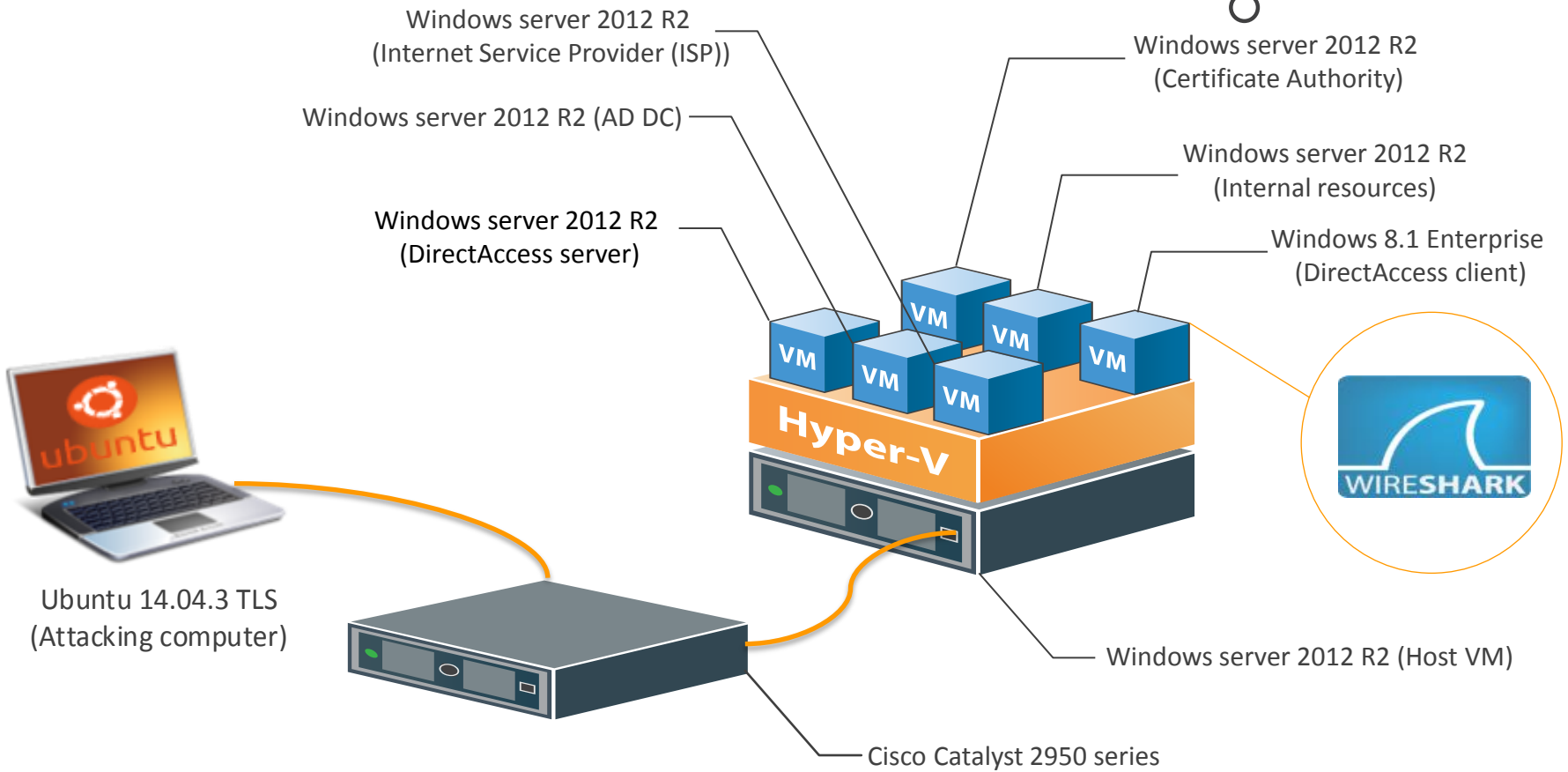


Figure 3 DirectAccess lab components

DirectAccess configuration

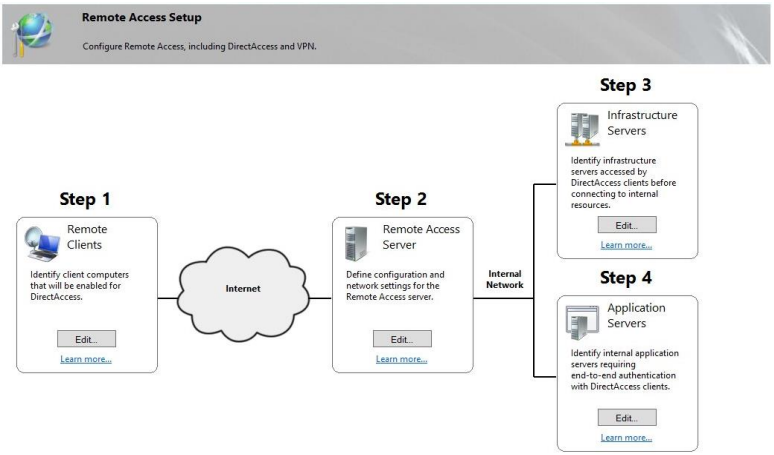


Figure 4 Screenshot for the configuration panel of DirectAccess

- Full access model
- DirectAccess server is an edge topology
- The DirectAccess computers are assigned to a security group
- The IPv6 tunneling is IP-HTTPS
- All the certificates are issued by the corpnet Certificate Authority (CA)
- IPSEC Encapsulated Security Payload (ESP) protocol tunnel mode
- Windows 8.1 uses Null cipher suites for IP-HTTPS

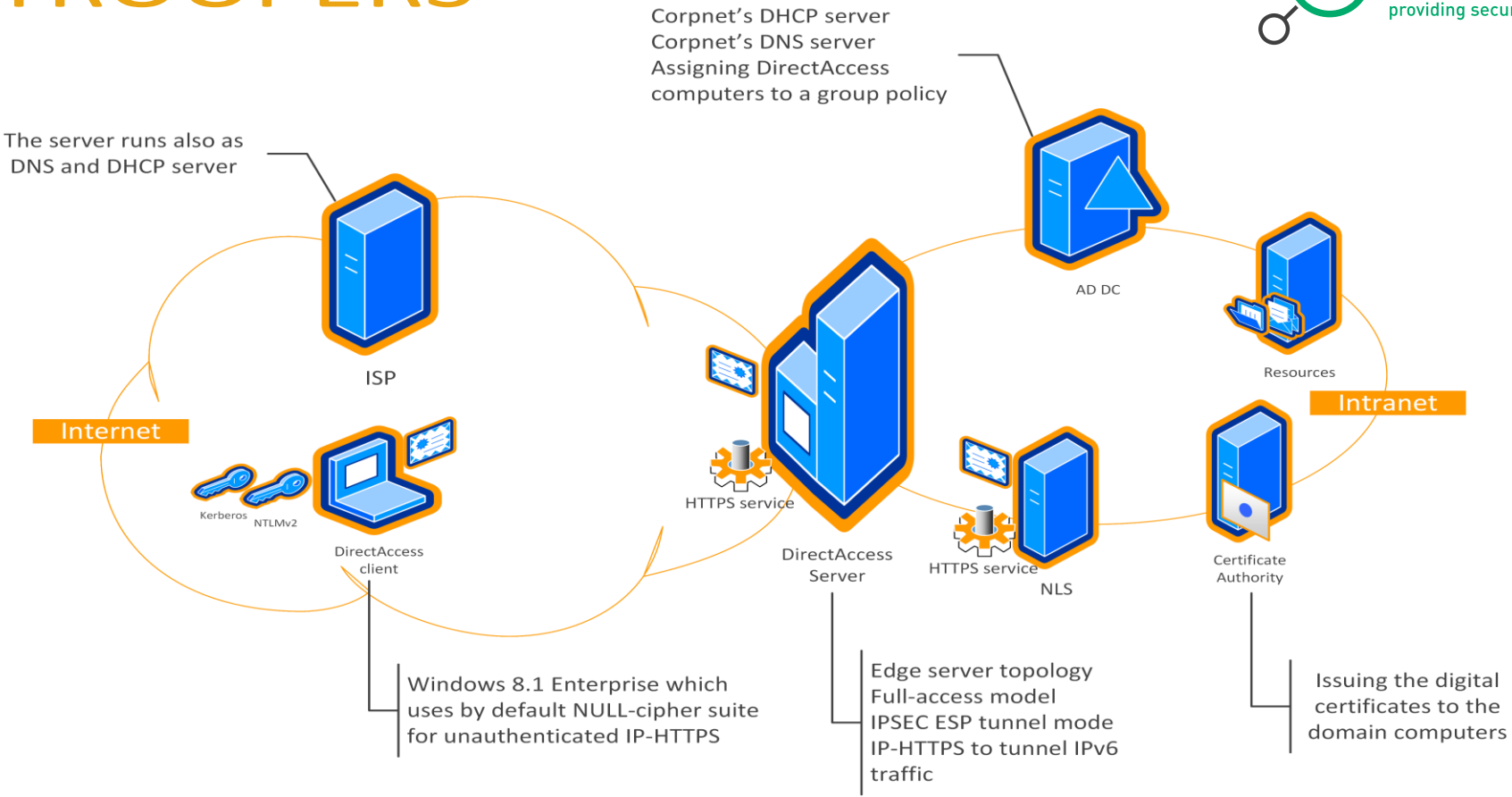


Figure 5 DirectAccess lab topology

Assessment

Scenarios and Attacker

- Two different scenarios were assessed:
  - IP-HTTPS default configuration
  - Authenticated IP-HTTPS
- Attacker knowledge and capabilities:
  - URL/IP of the DirectAccess server
  - Compromised or a trusted certificate
  - Position of attacker is remotely settled or within the local subnet of the client

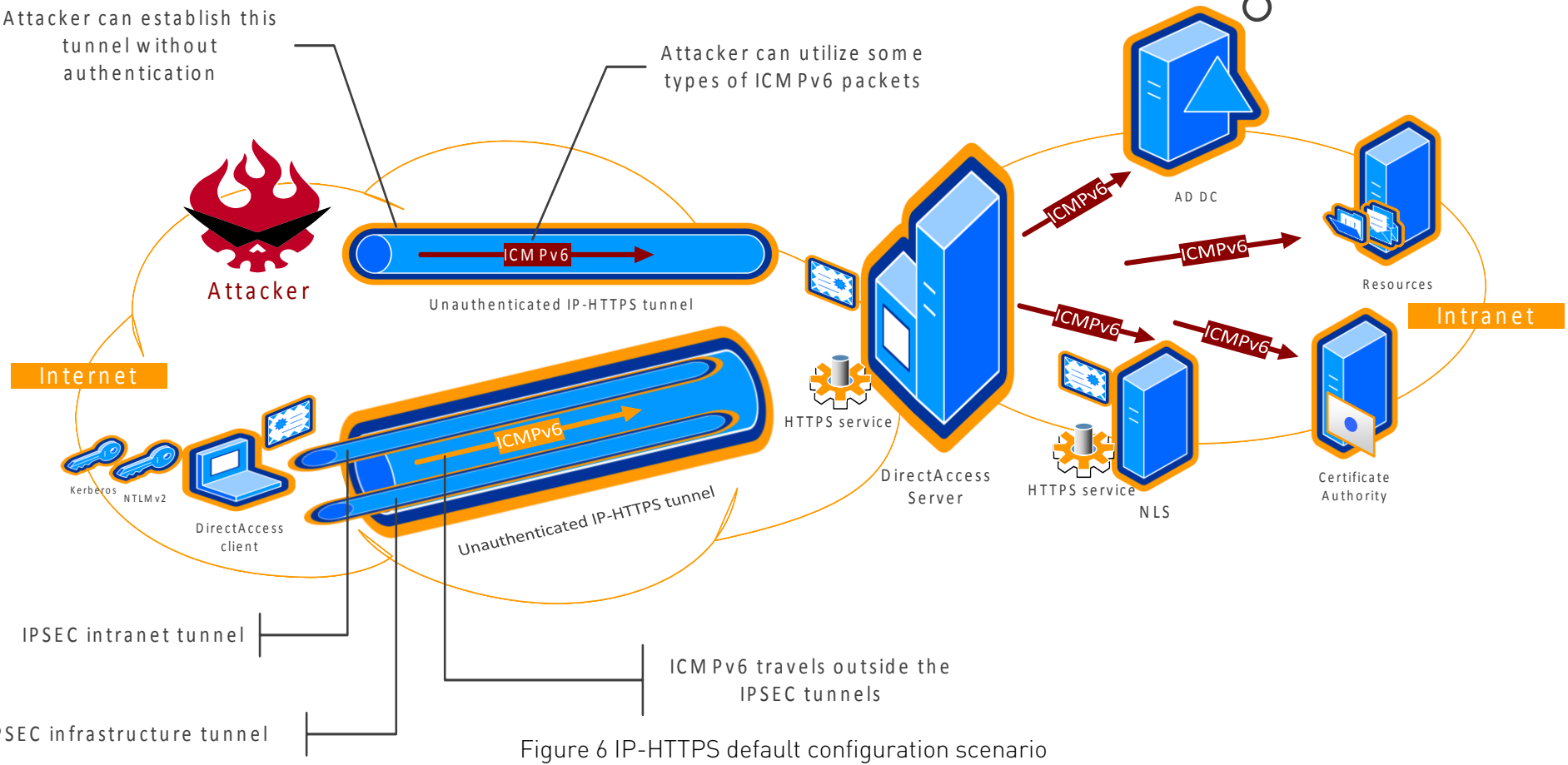


Figure 6 IP-HTTPS default configuration scenario

IP-HTTPS using Python

- The IP-HTTPS tunnel was established
- The internal servers were reachable using ICMPv6 echo request

```
DirectAccess@Lab: sudo python pyiphttps.py  corp-APP1-CA.pem edge1.da-lab.com

tun device created

[+] Socket was successfuly created
[+] A request was sent to the DirectAccess server
[+] A response was received from DirectAccess
[+] The session was opened without a client certificate

******* ICMPv6 packet was sent to ff02::2
******* ICMPv6 packet was received from fe80::4d27:bf21:36ce:1906
```

Figure 7 Using Ubuntu and Python IP-HTTPS interface to connect to the DirectAccess server

IP-HTTPS using Python

- The IP-HTTPS tunnel was established
- The internal servers were reachable using ICMPv6 echo request

```
DirectAccess@Lab: ifconfig
PyIP-HTTPS0 Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-
00-00
          inet6 addr: 2001:db8:1:1000:a60b:7ea2:10b1:6077/64 Scope:Global
          inet6 addr: 2001:db8:1:1000:d37:e431:ba56:309c/128 Scope:Global
          inet6 addr: fe80::a60b:7ea2:10b1:6077/128 Scope:Link
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1280  Metric:1
          RX packets:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:168 (168.0 B)  TX bytes:48 (48.0 B)
```

Figure 8 Python IP-HTTPS was configured with IPv6 addresses

Performed Attacks

- The unauthenticated IP-HTTPS:
  - Packets with multicast destination addresses are not forwarded
  - Packets with unicast addresses are not forwarded
  - Server replies on behalf of clients, if a client wants to configure an address that is already configured

L	Attack	Attacker position
1	Scan alive hosts using Ping scan	Local or remote
2	Scan for alive DA clients using Duplicate Address	Local or remote
3	Send packets with spoofed IPv6 addresses	Local or remote
4	Denial of Service against IP-HTTPS tunnel	Local or remote
5	Neighbor Cache exhaustion	Local or remote
6	MITM using a trusted certificate	Local or remote
7	MITM by relaying IPSEC packets via attacker's computer	Local

Table 1 Attacks that were performed on the unauthenticated IP-HTTPS tunnel

spoofing attack

```
DirectAccess@Lab: ifconfig PyIP-HTTPS0
PyIP-HTTPS0 Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet6 addr: 2001:db8:1:1000:7f88:dff:2b53:523b/64 Scope:Global
          inet6 addr: fe80::7f88:dff:2b53:523b/128 Scope:Link
          inet6 addr: 2001:db8:1:1000:ae9c:a83:34c8:97da/128 Scope:Global
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1280  Metric:1
          RX packets:23 errors:0 dropped:0 overruns:0 frame:0
          TX packets:25 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:2680 (2.6 KB)  TX bytes:1936 (1.9 KB)

DirectAccess@Lab: sudo python chiron_scanner.py -tun PyIP-HTTPS0 -s 2001:db8:1:1000:2848:6ae5:d308:a2cd
 -d 2001:db8:1::4 -sn
The MAC address of your sender is: False
The IPv6 address of your sender is: 2001:db8:1:1000:2848:6ae5:d308:a2cd
The interface to use is PyIP-HTTPS0
Starting sniffing...
Sniffer filter is ip6 and dst 2001:db8:1:1000:2848:6ae5:d308:a2cd and icmp6
System's default gateway for interface PyIP-HTTPS0 not found, or there are two default gateways
If you need to use a gateway, you must define it on your own
Let's start scanning
Press Ctrl-C to terminate before finishing
```

Figure 9 A packet with a spoofed source address

spoofing attack

ate Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
5 PM 11/6/2015	3.4485890		2001:DB8:1:1000:2848:6AE5:D308:A2CD	2001:DB8:1:0:0:0:0:4	ICMPv6	ICMPv6:Echo request, ID = 0xS
5 PM 11/6/2015	3.4543446		2001:DB8:1:0:0:0:0:4	2001:DB8:1:1000:2848:6AE5:D308:A2CD	ICMPv6	ICMPv6:Echo reply, ID = 0x9c3
5 PM 11/6/2015	3.4473567	System	131.107.0.100	EDGE1	TLS	TLS:TLS Rec Layer-1 SSL Applica
5 PM 11/6/2015	3.4549766	System	EDGE1	DACLIENT3	TLS	TLS:TLS Rec Layer-1 SSL Applica
5 PM 11/6/2015	3.5023808	System	DACLIENT3	EDGE1	TCP	TCP:[Segment Lost]Flags=...A.

Frame Details

```
Frame: Number = 6, Captured Frame Length = 139, MediaType = ETHERNET
Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[00-15-5D-4A
Ipv4: Src = 131.107.0.2, Dest = 131.107.0.102, Next Protocol = TCP,
Tcp: [Segment Lost]Flags=...AP..., SrcPort=HTTPS(443), DstPort=49160
TLSSSLData: Transport Layer Security (TLS) Payload Data
TLS: TLS Rec Layer-1 SSL Application Data
  TlsRecordLayer: TLS Rec Layer-1 SSL Application Data
    ContentType: SSL Application Data
    Version: TLS 1.2
    Length: 80 (0x50)
```

Hex Details

Decode As | Width | Prot Off: 5 (0x05) | Frame Off:

```
0020  00 66 01 BB C0 08 F2 93  .f.»À.ò
0028  38 40 AF CD F1 33 50 18  8@¯Íñ3P.
0030  00 FD A1 DF 00 00 17 03  .ý¡ß....
0038  03 00 50 60 00 00 00 00  ..P`....
0040  08 3A 7F 20 01 0D B8 00  .:▯ ..¸.
0048  01 00 00 00 00 00 00 00  ........
0050  00 00 04 20 01 0D B8 00  ... ..¸.
0058  01 10 00 28 48 6A E5 D3  ...(HjåÓ
0060  08 A2 CD 81 00 6E 0E 9C  .¢Í .n.
```

Figure10 DirectAccess server replied to the spoofed address

spoofing attack

ate Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
5 PM 11/6/2015	3.4485890		2001:DB8:1:1000:2848:6AE5:D308:A2CD	2001:DB8:1:0:0:0:0:4	ICMPv6	ICMPv6:Echo request, ID = 0xS
5 PM 11/6/2015	3.4543446		2001:DB8:1:0:0:0:0:4	2001:DB8:1:1000:2848:6AE5:D308:A2CD	ICMPv6	ICMPv6:Echo reply, ID = 0x9c3
5 PM 11/6/2015	3.4473567	System	131.107.0.100	EDGE1	TLS	TLS:TLS Rec Layer-1 SSL Applica
5 PM 11/6/2015	3.4549766	System	EDGE1	DACLIENT3	TLS	TLS:TLS Rec Layer-1 SSL Applica
5 PM 11/6/2015	3.5023808	System	DACLIENT3	EDGE1	TCP	TCP:[Segment Lost]Flags=...A.

Frame Details

```
Frame: Number = 6, Captured Frame Length = 139, MediaType = ETHERNET
Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[00-15-5D-4A
Ipv4: Src = 131.107.0.2, Dest = 131.107.0.102, Next Protocol = TCP,
Tcp: [Segment Lost]Flags=...AP..., SrcPort=HTTPS(443), DstPort=49160
TLSSSLData: Transport Layer Security (TLS) Payload Data
TLS: TLS Rec Layer-1 SSL Application Data
  TlsRecordLayer: TLS Rec Layer-1 SSL Application Data
    ContentType: SSL Application Data
    Version: TLS 1.2
    Length: 80 (0x50)
```

Hex Details

Decode As | Width | Prot Off: 5 (0x05) | Frame Off:

```
0020  00 66 01 BB C0 08 F2 93  .f.»À.ò
0028  38 40 AF CD F1 33 50 18  8@¯Íñ3P.
0030  00 FD A1 DF 00 00 17 03  .ý¡ß....
0038  03 00 50 60 00 00 00 00  ..P`....
0040  08 3A 7F 20 01 0D B8 00  .:▯ ..¸.
0048  01 00 00 00 00 00 00 00  ........
0050  00 00 04 20 01 0D B8 00  ... ..¸.
0058  01 10 00 28 48 6A E5 D3  ...(HjåÓ
0060  08 A2 CD 81 00 6E 0E 9C  .¢Í .n.
```

Figure10 DirectAccess server replied to the spoofed address

Neighbor Cache Exhaustion

- Windows server 2012 uses RFC 7048 "Neighbor Unreachability Detection Is Too Impatient"
- **Unreachable** state is maintained for a cache entry (CE)

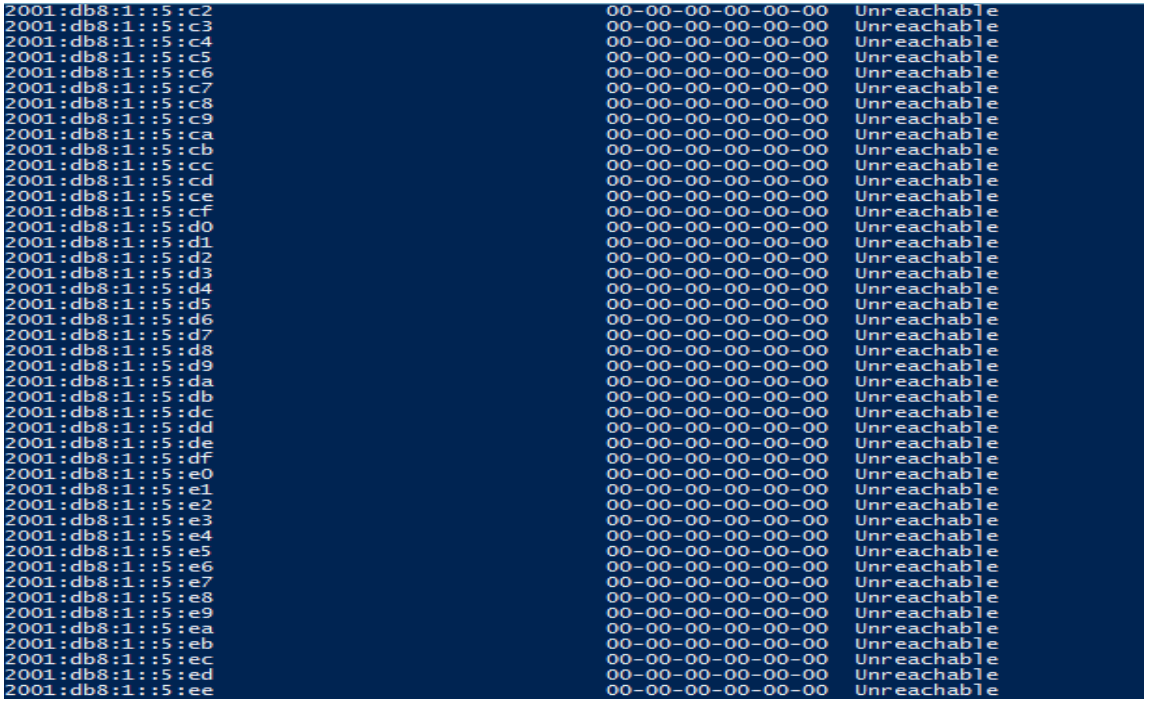


Figure11 DirectAccess server neighbor cache

Scan Connected DirectAccess Clients

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	::	ff02::1:ff08:a2cd	ICMPv6	64	Neighbor Solicitation for 2001:db8:1:1000
2	0.003406000	2001:db8:1:1000:2848:6ae5:d308:a2cd	ff02::1	ICMPv6	64	Neighbor Advertisement 2001:db8:1:1000:28
3	201.610669000	fe80::8455:62:c6a3:9a3a	ff02::1	ICMPv6	200	Router Advertisement

```
▸Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0
▸Raw packet data
▾Internet Protocol Version 6, Src: :: (::), Dst: ff02::1:ff08:a2cd (ff02::1:ff08:a2cd)
 ▸0110 .... = Version: 6
 ▸.... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
  .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 24
  Next header: ICMPv6 (58)
  Hop limit: 255
  Source: :: (::)
  Destination: ff02::1:ff08:a2cd (ff02::1:ff08:a2cd)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
▾Internet Control Message Protocol v6
  Type: Neighbor Solicitation (135)
  Code: 0
  Checksum: 0x9114 [correct]
  Reserved: 00000000
  Target Address: 2001:db8:1:1000:2848:6ae5:d308:a2cd (2001:db8:1:1000:2848:6ae5:d308:a2cd)
```

Figure12 Clients IPv6 enumeration using Duplicate Address Detection

Scan Connected DirectAccess Clients

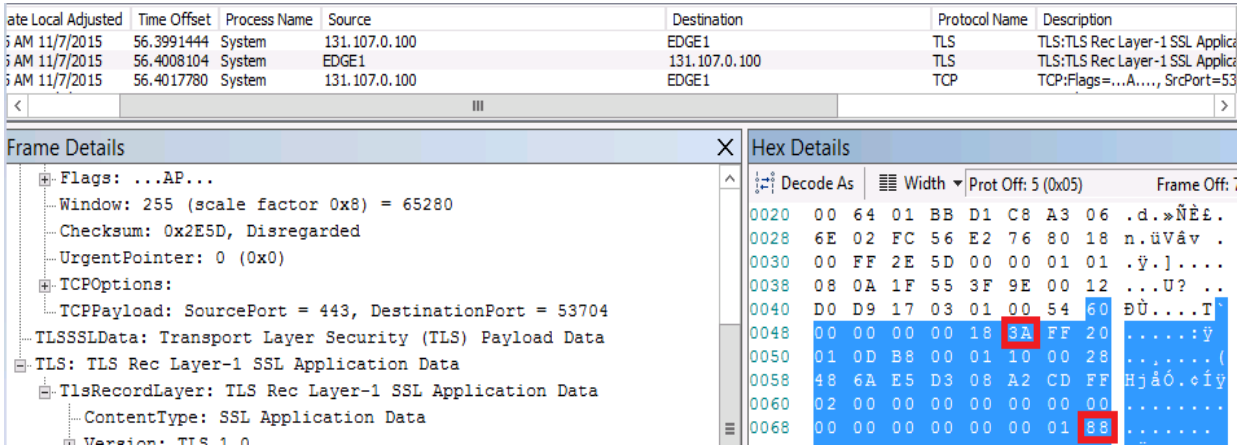


Figure13 DirectAccess server replied on behalf of the existing DirectAccess client

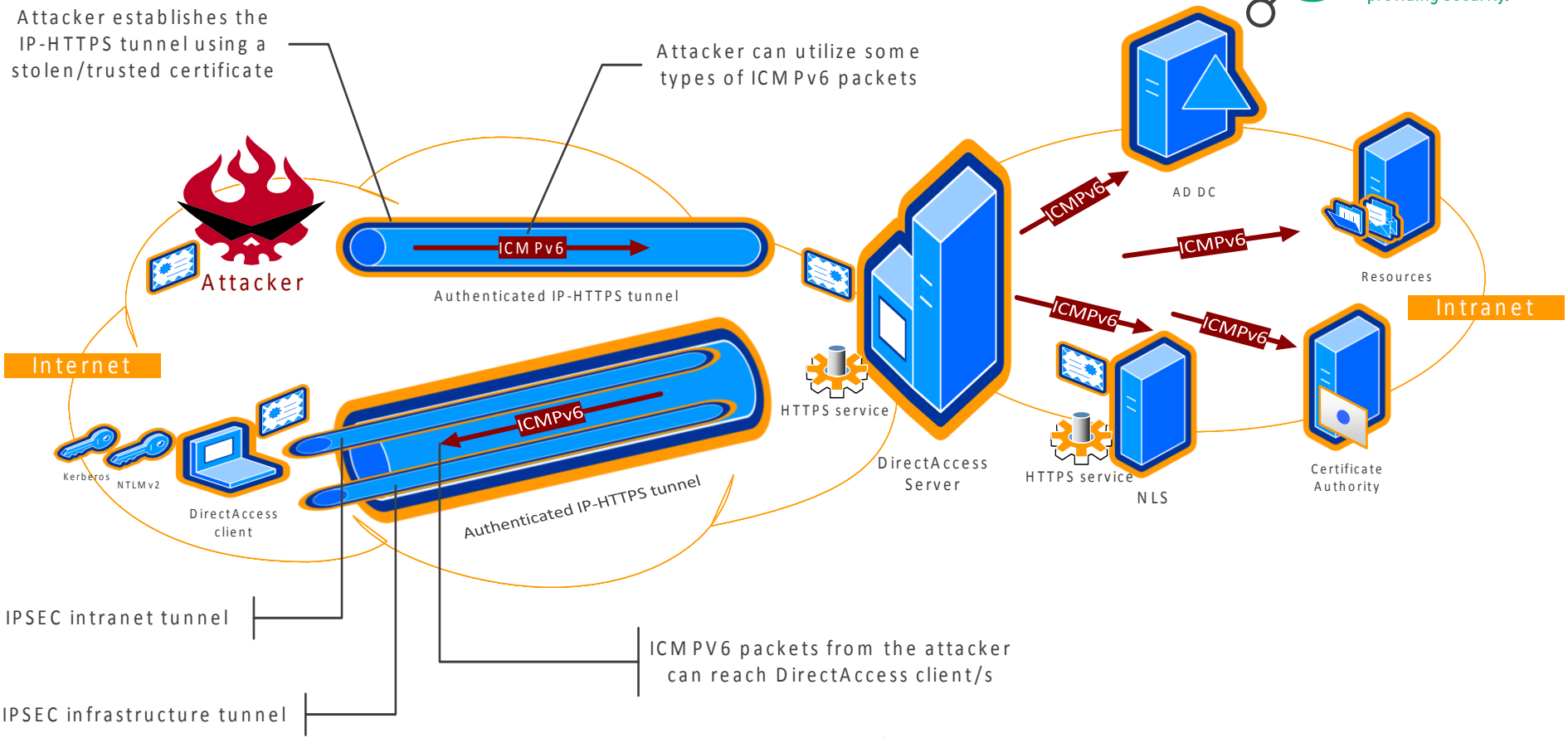


Figure 14 Authenticated IP-HTTPS scenario

Authenticated IP-HTTPS

- Almost all types of packets are accepted by the DirectAccess
- Null cipher suites can not be used any more

ⓘ DA client certificate was extracted using mimikatz

```
PS C:\Windows\system32> netsh interface httpstunnel set interface url=https://edge1.da-lab.com:443/IPHTTPS authmode=cert
ificates
Ok.

PS C:\Windows\system32> netsh interface httpstunnel show inter

Interface IPHTTPSInterface Parameters
------------------------------------------------------------
Role                        : server
URL                         : https://edge1.da-lab.com:443/IPHTTPS
Client authentication mode : certificates
Last Error Code             : 0x0
Interface Status            : IPHTTPS interface active
```

Figure 15 Configuring IP-HTTPS server component to use authentication

Authenticated IP-HTTPS

- Almost all types of packets are accepted by the DirectAccess
- Null cipher suites can not be used any more

ⓘ DA client certificate was extracted using mimikatz

```
PS C:\Windows\system32> netsh
netsh>http
netsh http>add sslcert ipport=131.107.0.2:443 certhash=9328f0dc1692a9e0699f3d6f9765e721a5200c18 appid={5d8e2743-ef20-4d3
8-8751-7e400f200e65} dsmapperusage=enable

SSL Certificate successfully added

netsh http>exit

PS C:\Windows\system32> netsh htt show sslcert

SSL Certificate bindings:
-------------------------

    IP:port                      : 0.0.0.0:443
    Certificate Hash             : 9328f0dc1692a9e0699f3d6f9765e721a5200c18
    Application ID               : {5d8e2743-ef20-4d38-8751-7e400f200e65}
    Certificate Store Name       : MY
    Verify Client Certificate Revocation : Enabled
    Verify Revocation Using Cached Client Certificate Only : Disabled
    Usage Check                  : Enabled
    Revocation Freshness Time    : 0
    URL Retrieval Timeout        : 0
    Ctl Identifier               : (null)
    Ctl Store Name               : (null)
    DS Mapper Usage              : Disabled
    Negotiate Client Certificate : Disabled

    IP:port                      : 131.107.0.2:443
    Certificate Hash             : 9328f0dc1692a9e0699f3d6f9765e721a5200c18
    Application ID               : {5d8e2743-ef20-4d38-8751-7e400f200e65}
    Certificate Store Name       : (null)
    Verify Client Certificate Revocation : Enabled
    Verify Revocation Using Cached Client Certificate Only : Disabled
    Usage Check                  : Enabled
    Revocation Freshness Time    : 0
    URL Retrieval Timeout        : 0
    Ctl Identifier               : (null)
    Ctl Store Name               : (null)
    DS Mapper Usage              : Enabled
    Negotiate Client Certificate : Disabled
```

Figure 16 Using certificate mapping to finish configuring authentication on IP-HTTPS tunnel

Authenticated IP-HTTPS

- Almost all types of packets are accepted by the DirectAccess
- Null cipher suites can not be used any more

ⓘ DA client certificate was extracted using mimikatz

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::4d27:bf21:36ce:1906	ff02::1:2	DHCPv6	150	Solicit XID: 0xd02c54
2	0.992911000	fe80::4d27:bf21:36ce:1906	ff02::1:2	DHCPv6	150	Solicit XID: 0xd02c54
3	2.000767000	fe80::4d27:bf21:36ce:1906	ff02::1:2	DHCPv6	150	Solicit XID: 0xd02c54
4	4.008571000	fe80::4d27:bf21:36ce:1906	ff02::1:2	DHCPv6	150	Solicit XID: 0xd02c54
5	8.015096000	fe80::4d27:bf21:36ce:1906	ff02::1:2	DHCPv6	150	Solicit XID: 0xd02c54
6	16.021458000	fe80::4d27:bf21:36ce:1906	ff02::1:2	DHCPv6	150	Solicit XID: 0xd02c54
7	32.033653000	fe80::4d27:bf21:36ce:1906	ff02::1:2	DHCPv6	150	Solicit XID: 0xd02c54
8	64.038054000	fe80::4d27:bf21:36ce:1906	ff02::1:2	DHCPv6	150	Solicit XID: 0xd02c54
9	227.777955000	fe80::2848:6ae5:d308:a2cd	ff02::1:2	DHCPv6	154	Solicit XID: 0xd003e
10	228.774611000	fe80::2848:6ae5:d308:a2cd	ff02::1:2	DHCPv6	154	Solicit XID: 0xd003e
11	229.776245000	fe80::2848:6ae5:d308:a2cd	ff02::1:2	DHCPv6	154	Solicit XID: 0xd003e
12	231.775204000	fe80::2848:6ae5:d308:a2cd	ff02::1:2	DHCPv6	154	Solicit XID: 0xd003e
13	235.775373000	fe80::2848:6ae5:d308:a2cd	ff02::1:2	DHCPv6	154	Solicit XID: 0xd003e
14	243.775780000	fe80::2848:6ae5:d308:a2cd	ff02::1:2	DHCPv6	154	Solicit XID: 0xd003e
15	259.775074000	fe80::2848:6ae5:d308:a2cd	ff02::1:2	DHCPv6	154	Solicit XID: 0xd003e
16	291.777375000	fe80::2848:6ae5:d308:a2cd	ff02::1:2	DHCPv6	154	Solicit XID: 0xd003e

Figure 17 Packets where received by Python IP-HTTPS interface on Ubuntu

Performed Attacks

- All the authenticated IP-HTTPS connections are trusted
- The only packets that are not forwarded those which have unspecified IPv6 source address "::"

L	Attack	Attacker position
1	Scan for alive DirectAccess clients using Ping scan	Local or remote
2	Scan DirectAccess clients for open ports	Local or remote
3	DoS against DirectAccess clients by sending fake Router Advertisement (RA) with randomized prefixes	Local or remote
4	Hijacking IPSEC packets that are sent to the client and cause a DoS	Local or remote
5	DoS DirectAccess client, by sending unsolicited Neighbor Solicitation (NS) with the IPv6 of the DirectAccess server as a source address	Local or remote

Table 2 Attacks that were performed on the authenticated IP-HTTPS tunnel

DoS with Fake RA

```
Tunnel adapter iphttpsinterface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:47a:4d9a:4b05:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:574:fd93:f3b6:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:db8:1:1000:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:ea5:6f16:4597:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:ef0:14d8:4bf1:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:10a8:b93e:7fea:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:12fc:679b:728:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:197c:d787:c7ad:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:19bb:7f85:735f:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:1d61:a334:39ef:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:1d76:e43c:9d78:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:1fe2:d044:8d4b:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:2126:d70c:f433:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:238e:180:6f92:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:23bd:bb89:229f:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:2534:5de:c0b7:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:276f:777:3788:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:2dcc:3d82:97e3:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:2ddb:c260:daeb:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:3410:db2f:b33a:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:3474:9b37:7d9c:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:37cc:e167:7891:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:40a7:10ae:19d6:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:4181:5729:a91:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:4386:83bb:9ad9:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:4437:9842:43dd:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:4952:379e:ddbb:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:4b98:38fb:b012:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:5237:5a74:ac5a:ccac:1fc6:9356:b1fe
   IPv6 Address. . . . . . . . . . . : 2001:5428:df19:903e:ccac:1fc6:9356:b1fe
```

Figure 18 Part of the addresses that were configured after receiving a fake RA with randomized prefixes

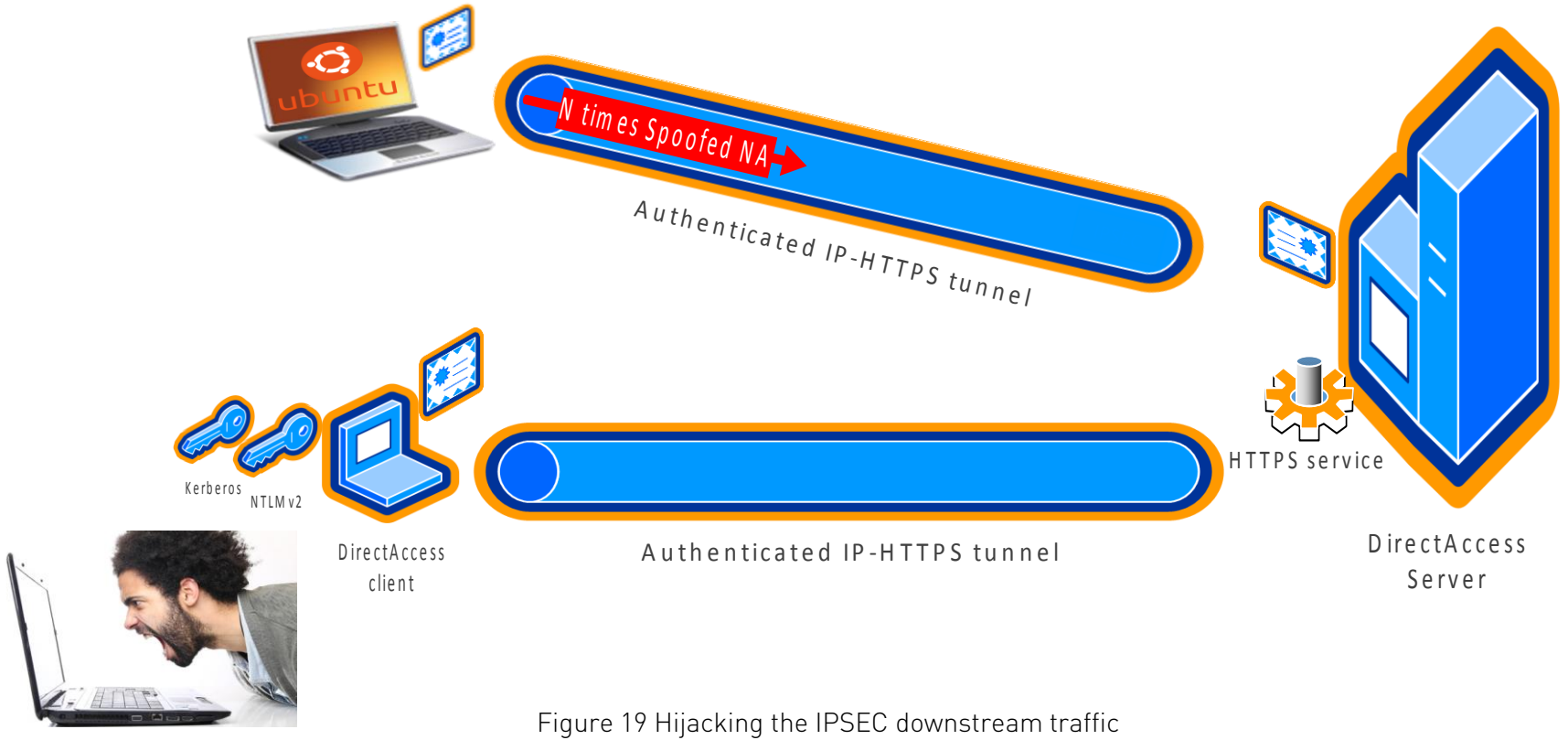


Figure 19 Hijacking the IPSEC downstream traffic

MITM The IP-HTTPS Traffic

No.	Time	Source	Destination	Protocol	Length	Info
284	2845.445045000	2002:836b:3::836b:3	2001:db8:1:1000:4d74:a9e1:7d8c:5104	ESP	140	ESP (SPI=0x3c477bfa)
285	2846.717855000	2001:db8:1:1000:4d74:a9e1:7d8c:5104	2001:db8:1:1000:4d27:bf21:36ce:1906	ICMPv6	64	Neighbor Advertisement
286	2847.455825000	2002:836b:3::836b:3	2001:db8:1:1000:4d74:a9e1:7d8c:5104	ESP	140	ESP (SPI=0x3c477bfa)
287	2847.978752000	2001:db8:1:1000:4d27:bf21:36ce:1906	2001:db8:1:1000:4d74:a9e1:7d8c:5104	ICMPv6	64	Neighbor Solicitation
288	2848.669770000	2001:db8:1:1000:4d74:a9e1:7d8c:5104	2001:db8:1:1000:4d27:bf21:36ce:1906	ICMPv6	64	Neighbor Advertisement
289	2848.978707000	2001:db8:1:1000:4d27:bf21:36ce:1906	2001:db8:1:1000:4d74:a9e1:7d8c:5104	ICMPv6	64	Neighbor Solicitation
290	2849.459945000	2002:836b:3::836b:3	2001:db8:1:1000:4d74:a9e1:7d8c:5104	ESP	140	ESP (SPI=0x3c477bfa)
291	2849.976979000	2001:db8:1:1000:4d27:bf21:36ce:1906	2001:db8:1:1000:4d74:a9e1:7d8c:5104	ICMPv6	64	Neighbor Solicitation
292	2850.645890000	2001:db8:1:1000:4d74:a9e1:7d8c:5104	2001:db8:1:1000:4d27:bf21:36ce:1906	ICMPv6	64	Neighbor Advertisement
293	2851.472781000	2002:836b:3::836b:3	2001:db8:1:1000:4d74:a9e1:7d8c:5104	ESP	140	ESP (SPI=0x3c477bfa)
294	2852.184671000	2002:836b:3::836b:3	2001:db8:1:1000:4d74:a9e1:7d8c:5104	ISAKMP	148	Unknown 246
295	2853.481285000	2002:836b:3::836b:3	2001:db8:1:1000:4d74:a9e1:7d8c:5104	ESP	140	ESP (SPI=0x3c477bfa)
296	2855.483893000	2002:836b:3::836b:3	2001:db8:1:1000:4d74:a9e1:7d8c:5104	ESP	140	ESP (SPI=0x3c477bfa)
297	2856.472017000	2001:db8:1:1000:4d27:bf21:36ce:1906	2001:db8:1:1000:4d74:a9e1:7d8c:5104	ICMPv6	64	Neighbor Solicitation
298	2857.475086000	2001:db8:1:1000:4d27:bf21:36ce:1906	2001:db8:1:1000:4d74:a9e1:7d8c:5104	ICMPv6	64	Neighbor Solicitation
299	2858.474930000	2001:db8:1:1000:4d27:bf21:36ce:1906	2001:db8:1:1000:4d74:a9e1:7d8c:5104	ICMPv6	64	Neighbor Solicitation
300	2863.125749000	2001:db8:1:1000:4d74:a9e1:7d8c:5104	2001:db8:1:1000:4d27:bf21:36ce:1906	ICMPv6	64	Neighbor Advertisement
301	2864.781805000	2001:db8:1:1000:4d74:a9e1:7d8c:5104	2001:db8:1:1000:4d27:bf21:36ce:1906	ICMPv6	64	Neighbor Advertisement
302	2866.617729000	2001:db8:1:1000:4d74:a9e1:7d8c:5104	2001:db8:1:1000:4d27:bf21:36ce:1906	ICMPv6	64	Neighbor Advertisement
303	2867.589819000	2002:836b:3::836b:3	2001:db8:1:1000:4d74:a9e1:7d8c:5104	ISAKMP	148	Unknown 246
304	2872.468796000	2001:db8:1:1000:4d27:bf21:36ce:1906	2001:db8:1:1000:4d74:a9e1:7d8c:5104	ICMPv6	64	Neighbor Solicitation
305	2873.476798000	2001:db8:1:1000:4d27:bf21:36ce:1906	2001:db8:1:1000:4d74:a9e1:7d8c:5104	ICMPv6	64	Neighbor Solicitation
306	2874.471074000	2001:db8:1:1000:4d27:bf21:36ce:1906	2001:db8:1:1000:4d74:a9e1:7d8c:5104	ICMPv6	64	Neighbor Solicitation
307	2882.599563000	2002:836b:3::836b:3	2001:db8:1:1000:4d74:a9e1:7d8c:5104	ISAKMP	148	Unknown 246

Figure 20 The attacking machine received IPSEC packets after a DirectAccess client was switched off

MITM The IP-HTTPS Traffic

Source	Destination	Protocol	Length	Info
2001:db8:1:1000:81ea:7491:e777:829	2001:db8:1:1000:4d27:bf21:36ce:1906	ICMPv6	64	Neighbor Advertisement
2001:db8:1:1000:81ea:7491:e777:829	2001:db8:1:1000:4d27:bf21:36ce:1906	ICMPv6	64	Neighbor Advertisement
2001:db8:1:1000:81ea:7491:e777:829	2001:db8:1:1000:4d27:bf21:36ce:1906	ICMPv6	64	Neighbor Advertisement
2002:836b:3::836b:3	2001:db8:1:1000:81ea:7491:e777:829	ISAKMP	148	Unknown 246
2002:836b:2::836b:2	2001:db8:1:1000:81ea:7491:e777:829	ISAKMP	148	Unknown 246
2001:db8:1:1000:81ea:7491:e777:829	2001:db8:1:1000:4d27:bf21:36ce:1906	ICMPv6	64	Neighbor Advertisement
2001:db8:1:1000:4d27:bf21:36ce:1906	2001:db8:1:1000:81ea:7491:e777:829	ICMPv6	64	Neighbor Solicitation
2001:db8:1:1000:4d27:bf21:36ce:1906	2001:db8:1:1000:81ea:7491:e777:829	ICMPv6	64	Neighbor Solicitation
2001:db8:1:1000:4d27:bf21:36ce:1906	2001:db8:1:1000:81ea:7491:e777:829	ICMPv6	64	Neighbor Solicitation
2002:836b:2::836b:2	2001:db8:1:1000:81ea:7491:e777:829	ESP	140	ESP (SPI=0x5d0cdd74)
2002:836b:2::836b:2	2001:db8:1:1000:81ea:7491:e777:829	ESP	140	ESP (SPI=0x5d0cdd74)
2002:836b:3::836b:3	2001:db8:1:1000:81ea:7491:e777:829	ESP	268	ESP (SPI=0xfb2e423c)
2002:836b:2::836b:2	2001:db8:1:1000:81ea:7491:e777:829	ESP	140	ESP (SPI=0x5d0cdd74)
2002:836b:3::836b:3	2001:db8:1:1000:81ea:7491:e777:829	ESP	268	ESP (SPI=0xfb2e423c)
2002:836b:2::836b:2	2001:db8:1:1000:81ea:7491:e777:829	ISAKMP	388	Unknown 244
2002:836b:3::836b:3	2001:db8:1:1000:81ea:7491:e777:829	ESP	268	ESP (SPI=0xfb2e423c)
2002:836b:2::836b:2	2001:db8:1:1000:81ea:7491:e777:829	ISAKMP	388	Unknown 244
2002:836b:2::836b:2	2001:db8:1:1000:81ea:7491:e777:829	ISAKMP	388	Unknown 244
2002:836b:3::836b:3	2001:db8:1:1000:81ea:7491:e777:829	ESP	268	ESP (SPI=0xfb2e423c)
2001:db8:1:1000:4d27:bf21:36ce:1906	2001:db8:1:1000:81ea:7491:e777:829	ICMPv6	64	Neighbor Solicitation
2001:db8:1:1000:4d27:bf21:36ce:1906	2001:db8:1:1000:81ea:7491:e777:829	ICMPv6	64	Neighbor Solicitation
2002:836b:2::836b:2	2001:db8:1:1000:81ea:7491:e777:829	ISAKMP	388	Unknown 244
2001:db8:1:1000:4d27:bf21:36ce:1906	2001:db8:1:1000:81ea:7491:e777:829	ICMPv6	64	Neighbor Solicitation
2002:836b:3::836b:3	2001:db8:1:1000:81ea:7491:e777:829	ESP	268	ESP (SPI=0xfb2e423c)

Figure 21 Sending spoofed NA's to the DirectAccess server and hijacking the connection from server to the client

MITM The IP-HTTPS Traffic

- Spoof the server RA
- Set the **Router Preference** flag with high priority
- Set all **Route Information** (RFC 4191) options with high priority
- Use the same advertised **Prefix Information**

```
225 22.0025369 fe80::8455:62:c6a3:ff02::1              ICMPv6   200 Router Advertisement
226 22.0026859 fe80::ccac:1fc6:935ff02::16             ICMPv6    76 Multicast Listener Report
227 22.0803366 ::                  ff02::1:ff56:b1fe   ICMPv6    64 Neighbor Solicitation for
228 22.0804302 ::                  ff02::1:ffa6:fea2   ICMPv6    64 Neighbor Solicitation for
    ..0. .... = Home Agent: Not set
    ...0 0... = Prf (Default Router Preference): Medium (0)
    .... .0.. = Proxy: Not set
    .... ..0. = Reserved: 0
  Router lifetime (s): 0
  Reachable time (ms): 0
  Retrans timer (ms): 0
⊟ ICMPv6 Option (MTU : 1280)
    Type: MTU (5)
    Length: 1 (8 bytes)
    Reserved
    MTU: 1280
⊞ ICMPv6 Option (Route Information : Medium 2001:db8:1::/48)
⊞ ICMPv6 Option (Route Information : Medium 2001:db8:1::/64)
⊞ ICMPv6 Option (Prefix information : 2001:db8:1:1000::/64)
⊞ ICMPv6 Option (Route Information : Low 2002::/16)
⊞ ICMPv6 Option (Route Information : Medium 2002:836b:2::/64)
⊞ ICMPv6 Option (Route Information : Medium 2002:836b:3::/64)
```

Figure 22 Router Advertisement (RA) sent by DirectAccess server

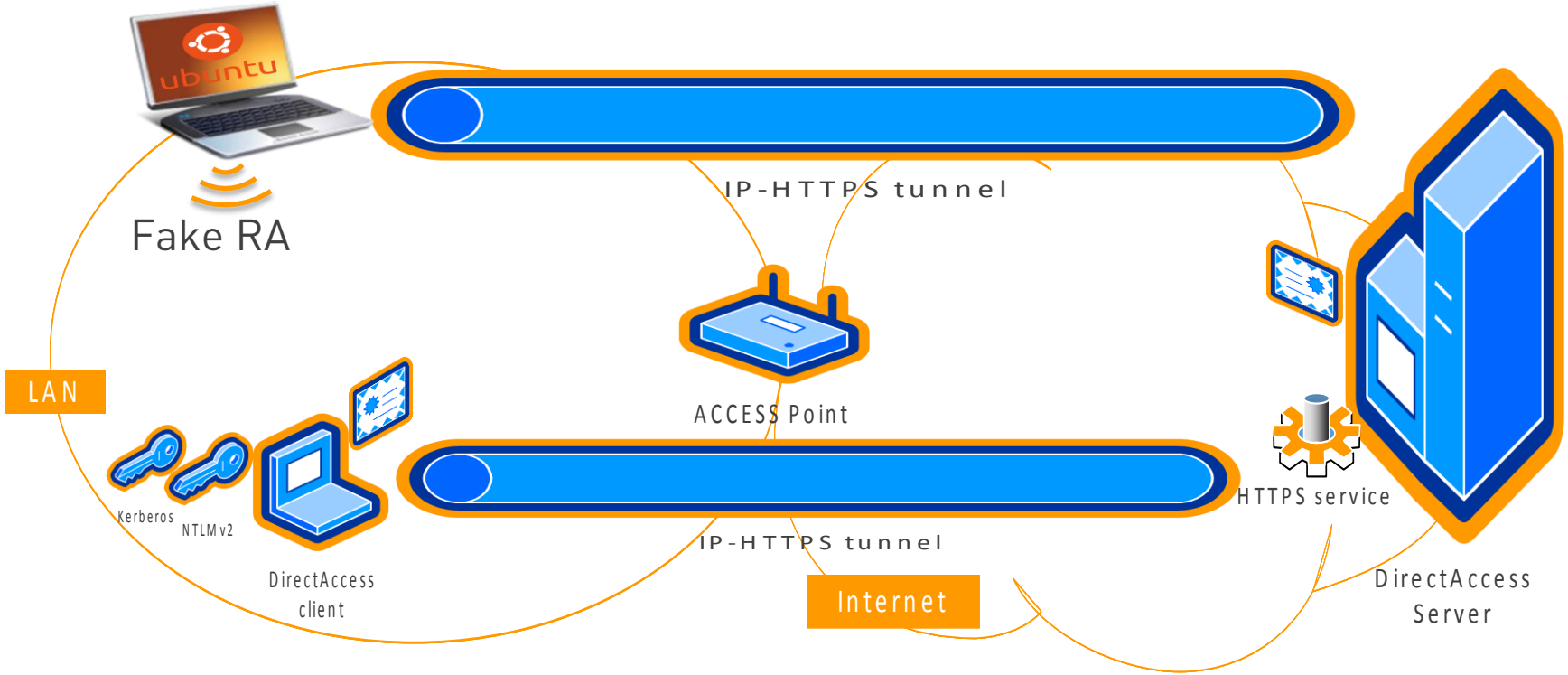


Figure 23 MITM on the local subnet

We've seen security bugs in almost everything: operating systems, applications programs, network hardware and software, and security products themselves. This is a direct result of the complexity of these systems. The more complex a system is--the more options it has, the more functionality it has, the more interfaces it has, the more interactions it has--the harder it is to analyze. Everything is more complicated: the specification, the design, the implementation, the use. And everything is relevant to security analysis.

Source: https://www.schneier.com/essays/archives/1999/11/a_plea_for_simplicit.html

Conclusion

- DirectAccess is a relatively new technology that offers the corpnet users a flexible, an always-on and an automatic access to the internal resources.
- The security assessment process showed that IP-HTTPS is a very critical component, which could be utilized by attackers to perform many IPv6 attacks on both DirectAccess client and server.
- The Thesis also pointed out the necessity of reviewing the configuration of both TLS and IPSEC protocol.
- The infrastructure tunnel and the 6to4 tunneling represent very attractive sources of attacks.