KAPITOLA 10

Nasazení protokolu IPv6 v sítích VPN pro vzdálený přístup

Tato kapitola se zabývá následujícími tématy:

- **Vzdálený přístup protokolu IPv6 pomocí klienta Cisco AnyConnect** – tato část se týká poskytování přístupu IPv6 pro podnikové služby prostřednictvím relace sítě VPN protokolu SSL s duální sadou protokolů pomocí klienta SSL Cisco AnyConnect VPN Client.
- **Vzdálený přístup protokolu IPv6 pomocí klienta Cisco VPN Client** – tato část diskutuje poskytování přístupu IPv6 pro podnikové služby prostřednictvím relace protokolu IPSec pomocí klienta Cisco VPN Client a hostitelských tunelů IPv6.

Mnoho IT oddělení věnuje značné úsilí poskytování přístupu IPv6 v rámci tradičních hranic svého podniku a často odkládá podporu uživatelů, kteří pracují na dálku. Tradiční šifrovaná klientská řešení sítí VPN (Virtual Private Network) lze využít k poskytování přístupu IPv6 pro vzdáleně pracující uživatele za předpokladu, že řešení sítě VPN dokáže nabídnout alespoň jednu z následujících tří možností:

- Lze přenášet protokol IPv6 přes relaci sítě VPN protokolů IPv4 a SSL (Secure Socket Layer) a zároveň je k dispozici podpora duální sady protokolů v terminačním zařízení sítě VPN.

- Lze používat tunely IPv6 v rámci navázané relace sítě VPN protokolů IPv4 a IPSec k terminačnímu bodu tunelu IPv6 uvnitř podniku.
- K dispozici je nativní podpora protokolu IPv6 mezi vzdáleným klientem a podnikovou sítí prostřednictvím zabezpečeného připojení (např. pomocí protokolu IPSec nebo SSL).

První řešení využívá klienta Cisco AnyConnect SSL VPN Client (SVC), který navazuje připojení protokolu SSL nad IPv4 k zařízení Cisco ASA (Adaptive Security Appliance). Protokol IPv6 je přenášen mezi klientem a zařízením ASA přes připojení IPv4/SSL a po terminaci na zařízení Cisco ASA je provoz protokolu IPv6 směrován ve formě nativních paketů IPv6.

Druhé řešení je založeno na klientovi Cisco VPN Client, který navazuje relaci protokolu IPSec nad IPv6 k jednomu z několika řešení Cisco VPN v ústředí, jako je zařízení Cisco ASA (Adaptive Security Appliance), směrovač Cisco IOS nebo koncentrátor Cisco VPN 3000. Pomocí mechanismu tunelování, jako je ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), 6to4 nebo tunely MCT, je provoz protokolu IPv6 zapouzdřen do paketů IPv4 a poté vložen do připojení sítě VPN protokolu IPSec. Zařízení Cisco VPN v ústředí ukončuje připojení protokolu IPSec, ale tunel IPv6 v IPv4 zůstává aktivní a je směrován k terminačnímu zařízení tunelu dále v podnikové síti. Po terminaci tunelu IPv6 v IPv6 je protokol IPv6 směrován formou nativních paketů IPv6.

Třetí současné řešení využívání možnosti technologie Microsoft DirectAccess (DA). Microsoft DA poskytuje funkce vzdáleného přístupu výhradně protokolem IPv6 mezi hostiteli se systémy Microsoft Windows 7 a Windows Server 2008 R2. Microsoft DA vyžaduje výhradní konektivitu protokolu IPv6 mezi zabezpečenými koncovými body. Pokud je transport mezi koncovými body zajištěn jiným protokolem než IPv6, technologie Microsoft DA se pokusí zapouzdřit pakety IPv6 pomocí některého mechanismu tunelování, jako je 6to4, Teredo, ISATAP a IP-HTTPS. Technologie Microsoft DA je poměrně složitá a její teorie, návrh a nasazení přesahují rozsah této kapitoly. Chcete-li zjistit, zda je vhodná pro vaši síť, přečtěte si průvodce na následující adrese společnosti Microsoft:

```
http://technet.microsoft.com/en-us/network/dd420463.aspx
```

Tato kapitola se zaměřuje na první dvě řešení: vzdálený přístup pomocí klientů Cisco AnyConnect a Cisco VPN Client. V době psaní této knihy ani jeden z nich nenabízí nativní podporu vzdáleného přístupu pomocí přenosu IPv6, ale u řešení AnyConnect se tato funkce plánuje. Zákaznický tým společnosti Cisco nebo stránky produktů na webu Cisco vám mohou poskytnout informace o tom, kdy bude k dispozici verze klienta AnyConnect pro přístup pomocí protokolu IPv6.

Vzdálený přístup protokolu IPv6 pomocí klienta Cisco AnyConnect

Pomocí řešení Cisco AnyConnect s firewallem Cisco ASA se uživatelé mohou bezpečně připojit k podnikové síti dvěma způsoby:

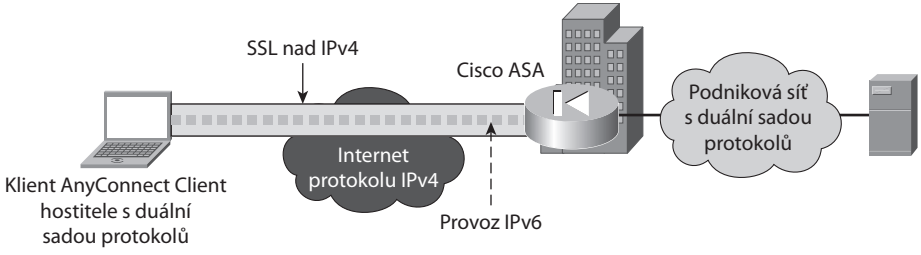
- Síť VPN protokolu SSL bez klienta
- Klient Cisco AnyConnect VPN Client

Metoda sítě VPN protokolu SSL bez klienta (také se označuje jako WebVPN) umožňuje, aby se uživatel z webového prohlížeče připojil k portálu firewallu Cisco ASA a navázal připojení TLS (Transport Layer Security) pomocí protokolu IPv4 a portu TCP číslo 443. Poté může klient přistupovat k aplikacím, které jsou umístěny v podnikové síti. Jestliže je firewall Cisco ASA s aplikacemi back-end, které jsou přístupné pomocí portálu, nakonfigurován pro připojení protokolem IPv6, může klient k příslušným aplikacím přistupovat tímto protokolem. Konfiguraci sítě VPN protokolu SSL bez klienta nebudeme v této kapitole uvádět. Další informace získáte v dokumentaci společnosti Cisco:

`http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html#wp1016526`

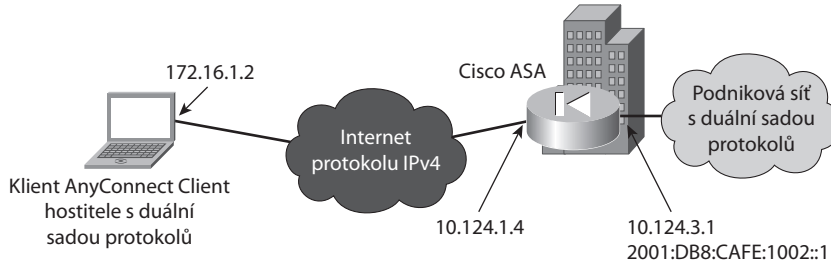
Cisco AnyConnect VPN Client je aplikace, která se instaluje do hostitelského systému uživatele. Uživatel spustí klienta Cisco AnyConnect VPN Client a naváže spojení DTLS (Datagram Transport Layer Security) pomocí protokolu IPv4 a portu UDP číslo 443 k firewallu Cisco ASA. Je sice podporováno i tradiční připojení TLS pomocí portu TCP číslo 443, ale metoda DTLS (RFC 4347) pomáhá odstranit potíže s latencí a šířkou pásma, které se běžně vyskytují u některých připojení protokolu SSL, protože poskytuje trasu protokolu UDP s nízkou latencí. To je výhodou u aplikací citlivých na latenci, jako je přenos hlasu. Když je v prostředí Cisco AnyConnect povolena metoda DTLS, používají se dva souběžné tunely: jeden pro TLS a druhý pro DTLS. Pokud je tunel UDP blokován nebo přerušen, může provoz procházet tunelem typu TLS.

Obrázek 10.1 představuje globální pohled na počítač s podporou duální sady protokolů, který přistupuje k podnikové síti pomocí klienta SVC. Klient SVC naváže relaci DTLS (přes Internet protokolu IPv4) k firewallu Cisco ASA. Firewall Cisco ASA rovněž podporuje funkčnost duální sady protokolů. Když pakety IPv6 projdou od klienta připojením DTLS k firewallu Cisco ASA, jsou směrovány do svého cíle v podnikové síti.



Obrázek 10.1: Připojení klienta Cisco AnyConnect VPN Client

Obrázek 10.2 znázorňuje ukázkovou topologii konfigurace popsané v této části. Klient má IPv4 adresu 172.16.1.2 a je připojen k Internetu protokolu IPv4. Firewall Cisco ASA se k Internetu protokolu IPv4 připojuje pomocí směrovače Cisco (není zobrazen), který poskytuje přístup, základní filtrování a překlad adres NAT (Network Address Translation) protokolu IPv4. Zařízení Cisco ASA má „vnější" IPv4 adresu 10.124.1.4 a „vnitřní" IPv4 adresu 10.124.3.1. Zařízení Cisco ASA má na vnitřní straně povolenu duální sadu protokolů a používá také IPv6 adresu 2001:DB8:CAFE:1002::1.



Obrázek 10.2: Ukázka topologie klienta Cisco AnyConnect VPN Client

Firewall Cisco ASA má dva fondy adres pro příchozí připojení klientů AnyConnect. Jeden fond obsahuje IPv4 adresy v rozsahu 10.124.3.30–10.124.3.80. Druhý je fond IPv6, který poskytuje 50 adres s prefixem 2001:DB8:CAFE:1002::/64 počínaje adresou 2001:DB8:CAFE:1002::100/64. Po navázání připojení klienta Cisco AnyConnect Client dostane klient přiřazenu IPv4 a IPv6 adresu z těchto fondů. Lze také využít jiné síťové služby nad protokoly IPv4 nebo IPv6, jako je DNS (Domain Name System), autorizace a autentizace uživatelů, integrace služby Microsoft Active Directory atd. Bezpečnostní filtrování a kontrola se v tomto modelu neliší od modelu s výhradní podporou protokolu IPv4. Zásady zabezpečení provozu směřujícího do interní sítě se u protokolu IPv6 aplikují na stejném místě jako v případě protokolu IPv4.

Konfigurace v příkladu 10.1 představuje výsek z kompletní konfigurace firewallu Cisco ASA a není určena jako vzor optimální konfigurace. Jedná se pouze o příklad toho, jak povolit podporu protokolu IPv6 pro klienta Cisco AnyConnect. Všimněte si také, že celou tuto konfiguraci lze provést v grafickém uživatelském rozhraní správce Cisco ASDM (Adaptive Security Device Manager).

V příkladu je patrné, že existuje „vnější“ a „vnitřní“ rozhraní. Software Cisco ASA vyžaduje povolení základní podpory protokolu IPv6 (příkazem **ipv6 enable**) na vnějším rozhraní. Jedná se pouze o požadavek softwaru a toto rozhraní nezpracovává pakety IPv6 v relaci sítě VPN. Ochrana tohoto rozhraní před útoky protokolu IPv6 z Internetu nevyžaduje žádná bezpečnostní opatření, protože tento příkaz je lokálně významný (ačkoli vzniká linková lokální IPv6 adresa) a není k dispozici žádný přístup protokolem IPv6 (internetové připojení využívá výhradně protokol IPv4). Aby měl útočník minimální šanci zaútočit na linkovou lokální adresu vnějšího rozhraní, potřeboval by přímý fyzický přístup k této lince nebo portu.

Příklad 10.1: Konfigurace připojení AnyConnect u firewallu Cisco ASA

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.124.1.4 255.255.255.0
 ipv6 enable                 #Software vyžaduje povolení protokolu IPv6 na
                             #vnějším rozhraní

!
interface GigabitEthernet0/1
 nameif inside
```

```
 security-level 100
 ip address 10.124.3.1 255.255.255.0
 ipv6 address 2001:db8:cafe:1002::1/64

!
ip local pool v4Pool 10.124.3.30-10.124.3.80 mask 255.255.255.0
ipv6 local pool v6Pool 2001:db8:cafe:1002::100/64 50  #fond v6 (50 adres)

ipv6 route inside ::/0 2001:db8:cafe:1002::3          #výchozí trasa směřuje na
                                                      #další přeskok v podnikové
                                                      #síti

!
route outside 0.0.0.0 0.0.0.0 10.124.1.1 1
!
webvpn
 enable outside
 svc image disk0:/anyconnect-win-2.4.1012-k9.pkg 1
 svc enable
group-policy ANYCONNECTGRP internal
group-policy ANYCONNECTGRP attributes

 vpn-tunnel-protocol svc webvpn          #Povolení klienta SSL VPN Client
                                         #a připojení bez klienta

 split-tunnel-policy tunnelall           #Zákaz rozděleného tunelování

 webvpn
  svc dtls enable                        #Povolení DTLS (TLS nad UDP)

  svc keep-installer installed
  svc ask enable default svc timeout 15
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol IPSec l2tp-ipsec svc webvpn
 address-pools value v4Pool
 ipv6-address-pools value v6Pool

webvpn
  svc ask enable default svc timeout 15
username sslvpn1 password bzN3HgmMqoLp3Liy encrypted

username sslvpn1 attributes             #Přidružení testovacího uživatele
                                        # k zásadám skupin

 vpn-group-policy ANYCONNECTGRP

tunnel-group DefaultRAGroup general-attributes
 address-pool v4Pool
tunnel-group DefaultWEBVPNGroup general-attributes
 address-pool v4Pool
tunnel-group ANY-TG type remote-access
```

```
tunnel-group ANY-TG general-attributes      #Přiřazení zásad fondu či skupiny ke
                                            #skupině tunelů

 address-pool v4Pool

 ipv6-address-pool v6Pool

 default-group-policy ANYCONNECTGRP
```

Když klient naváže aktivní připojení SVC k firewallu Cisco ASA, lze pomocí několika výstupních příkazů zobrazit stav relace a statistiky. Příklad 10.2 představuje výstup dvou různých příkazů.

První výstup obsahuje název fondu IPv6, rozsah adres, velikost a počet adres, které se používají a které jsou k dispozici. Výstup informuje o používaných adresách „In Use" a dostupných adresách „Available Addresses" (výstup je zkrácen, protože seznam je velmi dlouhý).

Druhý výstup shrnuje výstup pro podrobnosti **vpn-sessiondb** zejména ohledně stavu tunelu DTLS. Výstup zahrnuje přiřazené IPv4 a IPv6 adresy a veřejnou IPv4 adresu, pomocí které se klient připojuje.

Příklad 10.2: Fond IPv6 a výstup příkazu **vpn-sessiondb**

```
asa-1# show ipv6 local pool v6Pool
IPv6 Pool v6Pool
Begin Address: 2001:db8:cafe:1002::100

End Address: 2001:db8:cafe:1002::131

Prefix Length: 64
Pool Size: 50

Number of used addresses: 2
Number of available addresses: 48

In Use Addresses:
2001:db8:cafe:1002::100
2001:db8:cafe:1002::101
Available Addresses:
2001:db8:cafe:1002::102
2001:db8:cafe:1002::103
!VÝSTUP ZKRÁCEN

asa-1# show vpn-sessiondb detail svc
!SHRNUTÍ VÝSTUPU...
DTLS-Tunnel:
  Tunnel ID    : 6.3
  Assigned IP  : 10.124.3.30   Public IP    : 172.16.1.2

  Assigned IPv6: 2001:db8:cafe:1002::100

  Encryption   : AES128        Hashing      : SHA1
```

```
Encapsulation: DTLSv1.0       UDP Src Port : 4430

UDP Dst Port : 443            Auth Mode    : userPassword
Idle Time Out: 30 Minutes     Idle TO Left : 30 Minutes
Client Type  : DTLS VPN Client
Client Ver   : AnyConnect Windows 2.4.1012
Bytes Tx     : 8720           Bytes Rx     : 26074
Pkts Tx      : 109            Pkts Rx      : 303
Pkts Tx Drop : 0              Pkts Rx Drop : 0
```

Na obrázku 10.3 je znázorněna statistika klienta Cisco AnyConnect VPN Client pro dané připojení.

Obrázek 10.3: Statistika klienta Cisco AnyConnect Client

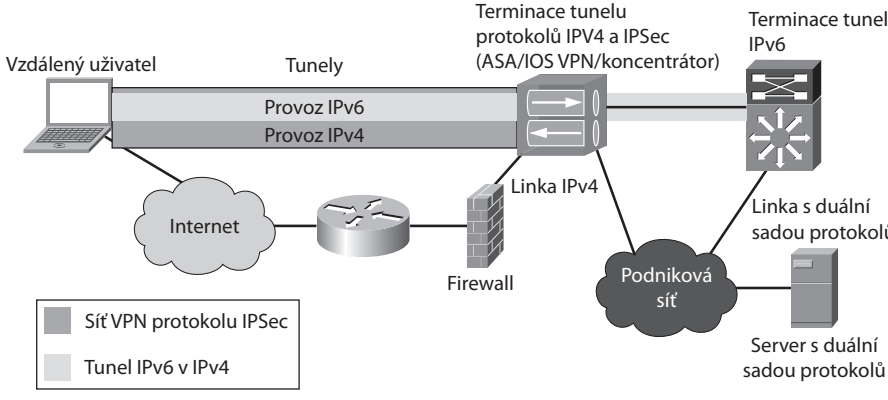
Uživatel nyní může z jediné relace klienta AnyConnect SSL přistupovat k aplikacím a službám protokolů IPv4 i IPv6. Podpora koncového přístupu protokolu IPv6 od uživatele k zařízení ASA v ústředí pomocí protokolu SSL nad transportem IPv6 je součástí cestovní mapy produktu a bude k dispozici zákazníkům, kteří ji potřebují.

Vzdálený přístup protokolu IPv6 pomocí klienta Cisco VPN Client

Klient Cisco VPN Client neposkytuje integrovanou podporu protokolu IPv6 jako řešení Cisco AnyConnect. Přesto lze zajistit podporu protokolu IPv6 prostřednictvím připojení klienta Cisco VPN Client pomocí hostitelských tunelů (dynamických či statických). Příkladem je

využití protokolu ISATAP (Intra-Site Automatic Tunnel Addressing Protocol – RFC 5214) u vzdáleného klienta spolu s navázaným připojením klienta Cisco VPN Client. ISATAP je hostitelský tunel, který poskytuje tunelovanou konektivitu protokolu IPv6 mezi hostitelem a směrovačem, přepínačem vrstvy 3 nebo serverem. Princip spočívá v tom, že po navázání připojení klienta Cisco VPN Client by měla existovat trasa směrování mezi hostitelem a koncovým bodem tunelu, který se nachází uvnitř podnikové sítě. Klient Cisco VPN Client umožňuje tunelovat provoz přes připojení protokolů IPv4 a IPSec.

Obrázek 10.4 znázorňuje ukázkovou topologii, kde se vzdálený uživatel připojuje k terminačnímu zařízení Cisco sítě VPN protokolu IPSec (např. Cisco IOS, ASA, koncentrátor 3000) prostřednictvím relace protokolů IPv4 a IPSec. Po navázání připojení je vytvořen tunel ISATAP (nebo tunel jiného hostitelského typu) mezi vzdáleným hostitelem a terminačním bodem tunelu IPv6 v podnikové síti. Po terminaci tunelu ISATAP lze provoz IPv6 směrovat do cíle pomocí duální sady protokolů nebo nativního připojení pouze protokolu IPv6. V tomto modelu je nutné seznamy řízení přístupu zabezpečení IPv6 a kontrolu aplikovat na provoz protokolu IPv6 po rozbalení v podnikové síti (tj. v interním terminačním bodě tunelu IPv6).



Obrázek 10.4: Použití klienta Cisco VPN Client s hostitelskými tunely

Poznámka

Kapitola 6, „Nasazení protokolu IPv6 v areálových sítích", obsahuje více podrobností týkajících se nasazení protokolu ISATAP a postupů, jak zajistit vysokou dostupnost příslušných tunelů v podnikové síti.

Příklad 10.3 představuje základní konfiguraci protokolu ISATAP nasazenou uvnitř podniku. U interního směrovače Cisco IOS nebo přepínače vrstvy 3, jako je např. Catalyst 6500 Supervisor 720, je definováno rozhraní tunelu. Je nakonfigurován prefix IPv6 a ID rozhraní používá upravenou adresu odvozenou z formátu EUI-64 (dle definice v dokumentu RFC 4291). Prefix použije klient ISATAP po svém připojení. Tunely v systému Cisco IOS mají ve výchozím nastavení zakázáno oznámení směrovače (RA – router advertisement). Vzhledem k tomu, že tunel se bude připojovat k více koncovým bodům, které potřebují informaci o prefixu IPv6, je nutné oznámení směrovače odesílat. Lze to zajistit vypnutím jejich výchozího potlačení. Zdrojem tunelu je zpětná smyčka u směrovače a tunel nemá žádný cíl, protože režim tunelu „isatap" označuje funkčnost tunelu s více připojenými body.

Poznámka

Není uvedena konfigurace terminačního zařízení sítě VPN, protože je z hlediska vlastního provozu protokolu IPv6 transparentní.

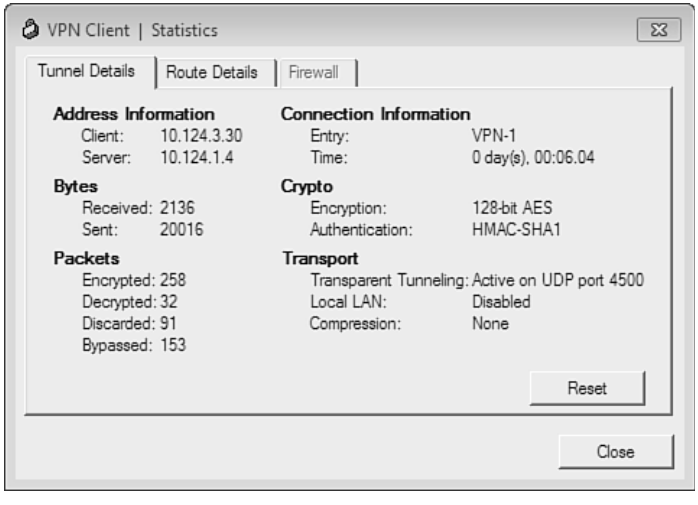
Příklad 10.3: Konfigurace protokolu ISATAP u klienta Cisco VPN Client

```
interface Loopback0
 ip address 10.124.109.1 255.255.255.255
!
interface Tunnel4
 no ip address
 no ip redirects
 ipv6 address 2001:DB8:CAFE:1009::/64 eui-64

 no ipv6 nd ra suppress

 tunnel source Loopback0

 tunnel mode ipv6ip isatap
```

Jak je vysvětleno v kapitole 6, protokol ISATAP může získat informace o směrovači ISATAP pomocí statické konfigurace nebo dynamicky z vyhledávání DNS. Doporučuje se pro začátek využít statickou konfiguraci, protože umožňuje jemnou kontrolu nad využitím tunelů ISATAP v podniku. Následující příkaz se používá v operačním systému Microsoft Windows a staticky identifikuje rozhraní směrovače (jeho rozhraní zpětné smyčky). Tento příkaz může přijímat IPv4 adresu nebo název hostitele (přeložený službou DNS). V tomto příkladu obsahuje příkaz **set router 10.124.109.1** IPv4 adresu nakonfigurovanou pro rozhraní Loopback0, které je zdrojem tunelu ISATAP.

```
C:\>netsh interface ipv6 isatap set router 10.124.109.1
Ok.
```

Z obrázku 10.5 je patrné, že klient používá relaci Cisco VPN Client a má adresu 10.124.3.30.



Obrázek 10.5: Relace klienta Cisco VPN Client

Příklad 10.4 obsahuje souhrnný výstup příkazu **ipconfig** zadaného v systému Microsoft Windows 7. Z výstupu lze zjistit, že klient má IPv6 adresu 2001:db8:cafe:1009:0:5e-fe:10.124.3.30. Hodnota 2001:db8:cafe:1009 je prefix definovaný u rozhraní Tunnel4 v příkladu 10.4. Řetězec 0:5efe identifikuje rozhraní ISATAP podle definice v dokumentu RFC 5214. Hodnota 10.124.3.30 je odvozena z IPv4 adresy klienta.

Příklad 10.4 také informuje o tom, že klient může úspěšně kontaktovat hostitele v podnikové síti příkazem ping.

Příklad 10.4: Výstup příkazů **ipconfig** a **ping** systému Microsoft Windows

```
Tunnel adapter isatap.cisco.com:

   Connection-specific DNS Suffix . : cisco.com
   IPv6 Address . . . . . . . . . . . : 2001:db8:cafe:1009:0:5efe:10.124.3.30

  Link-local IPv6 Address . . . . . : fe80::5efe:10.124.3.30%13
  Default Gateway . . . . . . . . . : fe80::5efe:10.124.109.1%13

C:\> ping 2001:db8:cafe:1005::1

Pinging 2001:db8:cafe:1005::1 with 32 bytes of data:
64 bytes from 2001:db8:cafe:1006::1: time=2ms
64 bytes from 2001:db8:cafe:1006::1: time<1ms
64 bytes from 2001:db8:cafe:1006::1: time=2ms
64 bytes from 2001:db8:cafe:1006::1: time=3ms
```

Shrnutí

Je nutné počítat s přístupem ke službám a aplikacím s podporou protokolu IPv6 z libovolného místa uvnitř i vně podniku. Funkce přístupu protokolu IPv6 přes řešení vzdálených sítí VPN postupně dozrávají. Společnost Cisco poskytuje přístup protokolu IPv6 pomocí klienta Cisco AnyConnect, který je založen na sítích VPN protokolu SSL, a toto řešení umožňuje přistupovat k podniku s použitím duální sady protokolů. Pokud se v současnosti využívá klient Cisco VPN Client nad protokolem IPSec, je vhodné přejít na řešení Cisco AnyConnect. Jestliže nelze v krátké době přejít na klienta Cisco AnyConnect a přitom je nutné zajistit přístup protokolu IPv6, lze nasadit hostitelské tunely (ISATAP, 6to4, MCT atd.), které zajišťují přístup vzdálených klientů prostřednictvím relace klienta Cisco VPN Client protokolu IPSec.

Další odkazy

Popoviciu, Ciprian P., Eric Levy-Abegnoli a Patrick Grossetete. *Deploying IPv6 Networks* (Nasazení sítí IPv6). Cisco Press, ISBN-10: 1-58705-210-5; ISBN-13: 978-1-58705-210-1.

Hogg, Scott a Eric Vyncke. *IPv6 Security* (Zabezpečení protokolu IPv6). Cisco Press, ISBN-10: 1-58705-594-5; ISBN-13: 978-1-58705-594-2.

Microsoft. Microsoft DirectAccess: http://technet.microsoft.com/en-us/network/dd420463.aspx.

Cisco. Cisco ASA 5500 SSL VPN Deployment Guide, Version 8.x (Příručka nasazení sítí VPN protokolu SSL u zařízení Cisco ASA 5500, verze 8.x): http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html.

Cisco. Cisco ASA 5500 SSL VPN Deployment Guide – Clientless SSL Documentation (Příručka nasazení sítí VPN protokolu SSL u zařízení Cisco ASA 5500 – dokumentace připojení SSL bez klienta): http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html#wp1016526.

Rescorla, E. a N. Modadugu. RFC 4347, „Datagram Transport Layer Security“ (Technologie DTLS).

Templin, F., T. Gleeson a D. Thaler. RFC 5214, „Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)“ (Tunely protokolu ISATAP – Intra-Site Automatic Tunnel Addressing Protocol).

Hinden, R. a S. Deering. RFC 4291, „IP Version 6 Addressing Architecture“ (Architektura adresování protokolu IPv6).