Openmachi

(Simulace LAN přes internet pomocí OpenVPN)

Pavel Hasenöhrl
hasenp1@fel.cvut.cz

ZADÁNÍ

Cílem je najít způsob, jak přes internet spojit počítače do virtuální sítě LAN s podporou toho, co přes internet obyčejně nejde (posílání broadcastů, IPX protokol) a případně vytvořit aplikaci, která toto řešení zastřeší. Jako cílová platforma je systém MS Windows XP.

Topologie sítě postačuje server-klient, ale za to řešení musí fungovat „všude“ (u serveru i klientů se předpokládá otevřený alespoň jeden TCP port) a síť musí být očíslovatelná libovolně. Dalším ukazatelem vhodnosti řešení je také bezpečnost.

POPIS ŘEŠENÍ

Jako referenční řešení byla brána aplikace Hamachi co se týče funkčnosti a jednoduchosti. Hamachi využívá VPN tunelů mezi všemi klientskými počítači, navíc inicializace spojení je v režii třetí strany, což je bezpečnostní riziko.

Výsledné řešení zcela jistě bude založeno na VPN technologii, nejlépe na již existující implementaci, která je dostupná na dané platformě k volnému použití a splňuje požadované vlastnosti. Systém MS Windows XP nabízí protokoly PPTP a L2TP, které taky nejsou vhodné pro tuto aplikaci (PPTP – bezpečnost, oba pak potřebují více portů). Jako ideální řešení se objevil program OpenVPN, který je navíc multiplatformní.

Program OpenVPN v tzv. ethernet bridging módu umožňuje posílání brodcastů, IPX protokol atd., je také znám díky své bezpečnosti, kterou zajišťuje knihovna OpenSSL. Pro svůj chod potřebuje pouze jeden TCP nebo UDP port (z pohledu klienta). Jedná se tzv. open source distribuovaný pod GPL licensí.

Nevýhoda ethernet bridging módu je jeho obtížnější zprovoznění na straně serveru. Je potřeba použít virtuální bridge k přemostění virtuálního TAP adaptéru využívaného OpenVPN a dalšího adaptéru, který má konektivitu do internetu. To je problém např, když je tomuto síťovému rozhranní přidělována adresa na základně MAC adresy (síťový most si vezme definovaným způsobem MAC adresu, kterou nelze jednoduše změnit). Ke všemu by server na okamžik ztratil konektivitu při přemosťování adaptérů. Zde mě napadlo řešit situaci překladem adres. Na serveru se vytvoří virtuální loopback adaptér, ten se přidá do přemostění s TAP adaptérem a na bridge se aplikuje NAT s překladem portů. Toto vše je možné provést jen pomocí zdrojů cílové platformy.

Lze tedy docílit požadovaného chování. Zbývá tedy řešení implementovat vhodnou aplikací.

APLIKACE

SPECIFIKACE

Aplikace musí usnadňovat konfiguraci serveru i klienta. Musí umožňovat spravování různých sítí. Součástí bude i automatizovaná bezpečná distruibuce certifikátů. Aplikace bude založena na již existujícím programovém vybavení (součásti systému a součásti distribuce OpenVPN).

ARCHITEKTURA

Standardní okenní aplikace typu WIN32. Je kladen důraz na co nejmenší závislosti na platformě

pro hlavní funkce aplikace. To je zařízeno sadou skriptů, které aplikace programově spouští v instanci programu cmd.exe. Skripty jsou uloženy v adresáři „scripts“.

Podstatnou část aplikace tvoří server a klient pro automatickou distribuci certifikátů. Celé to fukguje takto:

1) klient pošle svoje jméno a zašifrovanou výzvu
2) server rozšifruje výzvu a porovná ji
3) server odešle ca.crt
4) klient odešle svůj csr
5) server ho podepíše a odešle zpět jako crt

Celá tato komunikace je šifrovaná symetrickou šifrou (256b aes – cbc mód), klíč je odvozen z hesla, které si musí všichni účastníci sítě nějak sdělit mimo nezabezpečený kanál. K vlastnímu šifrování je použit program „openssl.exe“, ten se spouští na pozadí a s aplikací je propojen pomocí rour, zde bylo nutné použít další aplikaci „cat.exe“, která přeposílá data ze vstupu na výstup a skončí při obdržení řídicího znaku konce výstupu. To je nutné z toho důvodu, že data posílaná openssl musí být ukončena bez uzavření roury. Toto řešení není univerzální, lze tak šifrovat pouze tisknutelné znaky a znak „\n“, proto je ve skriptech pro šifrování uveden přepínač „-a“ (kódování base64).

Aplikace dále používá pro zjištění jména nově nainstalovaného adaptéru technologii WMI. Tato funkcionalita je přidána přímo v kódu prostřednictvím COM.

OVLÁDÁNÍ

Okno aplikace obsahuje hlavní menu, přes které se spouští všechny potřebné akce. V klientské oblasti je log událostí, kde se objevují důležitá hlášení o provedených akcích. V menu config jsou volby pro tvorbu nových sítí, načítání existující a upravování a ukládání aktuální konfigurace. Některé mají za následek, že se otevře dialog jen s editačními poli, které je nutné vyplnit. Dialog se potvrdí tlačítkem „OK“ nebo „Install“. Install má také za následek, že se nainstaluje nový adaptér daného typu s příslušným jménem. Tlačítko „Cancel“ potlačí provedené změny.

KONFIGURACE SÍTÍ

Každá síť má vlastní adresář, který obsahuje všechny potřebné soubory (certifikáty, klíče, konfigurační soubory atd.). Adresář má stejné jméno jako síť a musí být umísťěn ve stejném adresáři jako aplikace a neměl by se jmenovat jako adresář se skripty. Konfigurační soubor se jmenuje „config.txt“, má předepsaný formát „klíč=hodnota“ na každém řádku a používá kódování UCS–16. Není doporučeno měnit konfiguraci ručně, ale raději použít aplikaci.

DODATEK

Aplikace je v použitelném stavu, ale určitě by mohla být vylepšena. Ne totiž všechny operace ke zprovoznění serveru se daly jednoduše udělat programově nebo skriptem. Přidat adaptéry do přemostění lze totiž jednoduše pouze přes GUI. Také zajištění určitých služeb systému je složitější problém, který se musí zatím řešit ručně.

Jako další funkcionalitu, bych si představoval:

1) vylepšení logu (více informací, barevné rozlišení chyb…)
2) systém pro vizualizaci a správu klientů v síti (kdo právě komunikuje, kdo má klíč, možnost odstanění cetifikátu klienta na serveru…)