VŠB Technická univerzita Ostrava

Technologie Počítačových Sítí

SSL VPN

Obsah

Co je VPN

VPN (Virtual Private Network) je bezpečné (autentizované a šifrované) a přitom pro uživatele zcela transparentní spojení mezi dvěma či více sítěmi. Pro spojení mezi uživatelem a požadovanou destinací je použita veřejná síť (internet). Použitím pouze internetového prohlížeče mohou společnosti rozšířit jejich bezpečné podnikové sítě na libovolné místo v internetu jako jsou domácí počítače, internetové kiosky a bezdrátové přístupové body a tím zvýší produktivitu práce a umožní přístup do vnitřní sítě partnerům.

Typy VPN

Dnes existuje několik typů VPN technologie. Vzájemně se od sebe liší vrstvou architektury na které pracují. Nejrozšířenějším je standard VPN založený na *IPSec (Internet Protocol Security)*. Jedná se o rozšíření IP protokolu přinášející prvky zabezpečení. IPSec pracuje na třetí vrstvě ISO OSI modelu. Zabezpečuje přenášená data bez vazby na konkrétní aplikaci. Z hlediska protokolů vyšších vrstev je zcela transparentní. To přináší problém při realizaci IPSec VPN spojení přes firewally, ty totiž pracují na 3. vrstvě. VPN spojení musí být explicitně povolena. Pokud je výchozí politikou firewallu zahazovat všechna spojení, která nepatří do seznamů povolených (*DEFAULT DROP ALL*), což je správné, musí být VPN spojení zařazeno do seznamu povolených. Především se jedná o protokol UDP port 500 (IKE – Internet Key Exchange) a AH(Authentication header)/ESP(Encapsulating security payload) protokol.

Technologie IPSec VPN má ale i své nevýhody. První z nich je závislost VPN na jiných technologiích než jen IP. Tato nevýhoda může být překonána novým typem VPN sítí, pracujících na vyšších vrstvách ISO OSI architektury. Navíc, protože technologie IPSec je nezávislá na aplikacích, každý výrobce operačního software poskytuje produkty VPN řešení, které jsou často mezi sebou zcela nekompatibilní. A je zde i potenciální riziko průniku do vnitřní sítě zneužitím VPN koncentrátoru (prozrazení hesla, chybná konfigurace, ...).

Nejnovějším typem je VPN technologie založená na kombinaci symetrické a asymetrické kryptografie, nejčastěji nazývaná *VPN SSL (Virtual Private Network Secure Socket Layer)* pracující na L4 vrstvě.

SSL VPN

Termínem SSL VPN je označována řada často vzájemně nekompatibilních technologií. Nicméně, všechny jsou postaveny na stejné základní myšlence. Je jí využití asymetrické kryptografie a knihoven *SSL (Secure Socket Layer)* pro zašifrovanou komunikaci. Technologie protokolů rodiny *SSL/TLS (Transport Layer Security)* je dnes hojně využívána při šifrovaném přístupu k webovému serveru schématem HTTPS.

Cílem SSL VPN je vytvoření co nejtransparentnějšího šifrovaného tunelu, založeného na protokolu SSL. Vzhledem k přítomnosti SSL v běžných webových prohlížečích není nutné pro dosažení většiny nabízené funkčnosti instalovat na klientské počítače žádný speciální klientský software. K rozšíření možností SSL VPN řešení jsou dále používány malé aplikace v podobě Java appletů nebo ActiveX prvků. Právě bohatost nadstandardní výbavy významně ovlivňuje užitnou hodnotu implementací SSL VPN od různých výrobců.

Základní funkcionalita SSL VPN spočívá v zabezpečeném přístupu k vnitřním informačním zdrojům organizace. Je vytvořen SSL tunel mezi SSL VPN bránou a webovým prohlížečem na klientském počítači. SSL VPN brána se chová obdobně jako reverzní proxy. Požadavek od klienta je bránou přijat, ta jej přepošle na příslušný sever, který bráně vrátí odpověd, a ta ji odešle zpět dotazujícímu se klientovi. Komunikace mezi internetovým prohlížečem klienta a

bránou je zabezpečena silným šifrováním pomocí SSL knihovny. Požadavek od klienta je bránou přijat, ta jej přepošle na příslušný server, který bráně vrátí odpověď, a ta ji odešle zpět dotazujícímu se klientovi. Komunikace mezi webovým prohlížečem klienta a bránou je zabezpečena silným šifrováním pomocí SSL knihovny.

Úroveň zabezpečení komunikace mezi bránou a interním serverem zůstává nezměněna. V této podobě tedy může SSL VPN velmi dobře posloužit jako implementačně jednoduchý způsob, jak v rámci internetu zabezpečeně zpřístupnit webové portály informačních systémů organizace. Další běžnou vlastností SSL VPN řešení je možnost s pomocí bránou nabízeného webového rozhraní pracovat se soubory sdílenými v rámci vnitřní sítě pomocí CIFS, tedy sdílení souborů novějších systémů Windows, nebo unixového NFS.

SSL VPN versus IPSec VPN

SSL VPN pracuje s daty v TCP segmentech asociovaných s určitými porty. Z hlediska přenosu dat na síťové vrstvě je použití SSL zcela transparentní. Pomocí SSL je tedy možné zabezpečit obsah dat, nicméně další informace zapouzdřujícího protokolu síťové vrstvy (IP) už nijak dodatečně zabezpečeny nejsou.

To je v kontrastu s rozšířenou technologií IPSec, která poskytuje i výhody zabezpečení přenosu sítí (Internetem) a integritu dat. IPSec poskytuje mechanismus zabezpečení založený na 3. vrstvě. Velmi často jsou používány obě technologie ve vzájemné kombinaci pro dosažené maximální míry zabezpečení. Přes uvedené vlastnosti jsou SSL VPN technologie na postupu a jsou nasazovány v čím dál větší míře.

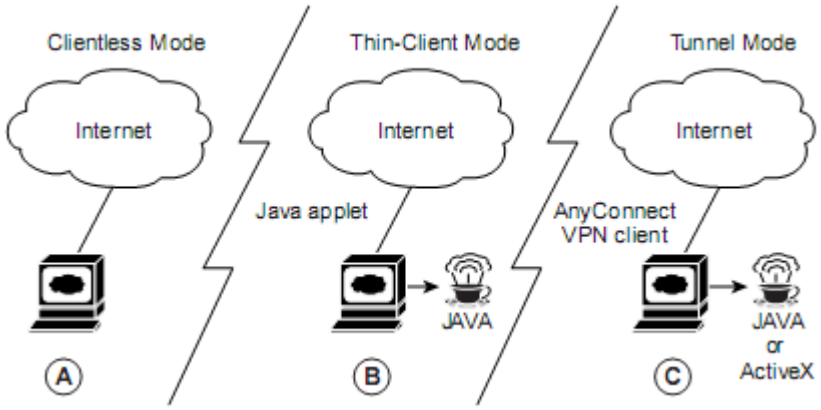
Typy SSL VPN

Mnoho produktů označovaných jako SSL VPN de facto nesplňuje definici virtuální privátní sítě. VPN technologie by správně měla poskytovat šifrované tunelové spojení mezi dvěma body sítě (počítači, sítěmi nebo počítačem a sítí). Nicméně SSL VPN technologie poskytují nejčastěji pouze SSL bránu (gateway), což úplně neodpovídá definici VPN. „Klasická“ VPN používající technologii IPSec přiděluje vzdálenému uživateli přístupová práva na základě ověření jeho autentizačních informací, tedy hesla, případně certifikátu. Pokud je uživatel autorizován k přístupu do vnitřní sítě, může fyzicky přistupovat ke všem zařízením ve vnitřní síti. Přístup k jednotlivým serverům a jejich aplikacím se musí řešit až na straně cílového stroje (serveru). VPN koncentrátor je z tohoto pohledu transparentní. Na druhou stranu dnešní rozsáhlá integrační řešení potřebují centralizovat správu přístupových práv pro jednotlivé uživatele a v nejlepším případě je přidělovat pro jednotlivé aplikace, nikoli celé servery, což na 3. vrstvě ISO/OSI není principielně možné. K tomu se přesně hodí SSL gateway (SSL VPN), pracující na vyšších vrstvách a má tedy možnost přidělovat přístupová práva na úrovni aplikace a navíc má možnost přistupovat k datovému obsahu. Navíc, k využití SSL VPN není třeba žádný specializovaný software na straně klienta, protože se vzdálenou SSL bránou je možné komunikovat HTTPS schématem a tedy přes standardní webový prohlížeč. Tím klesají výdaje nejen na software, ale i na vyškolení personálu. Existují 3 různé způsoby použití SSL VPN (zobrazeny na obr.1).

Vzdálený přístup

Uživatel se přihlásí a autentizuje přes http request v internetovém prohlížeči do zabezpečené brány. Tento proces vytvoří sezení s referencí na cookie. Po úspěšné autentizaci se uživateli zobrazí portálová stránka, která dovoluje přístup do vnitřní sítě. Všechny žádosti zaslané prohlížečem obsahují autentizační cookie. Portálová stránka

zobrazuje všechny zdroje dostupné ve vnitřní síti uživateli. Například poskytuje odkaz na stáhnutí java appletu pro přístup přes tenkého klienta.



Obr.1 Různé módy vzdáleného připojení

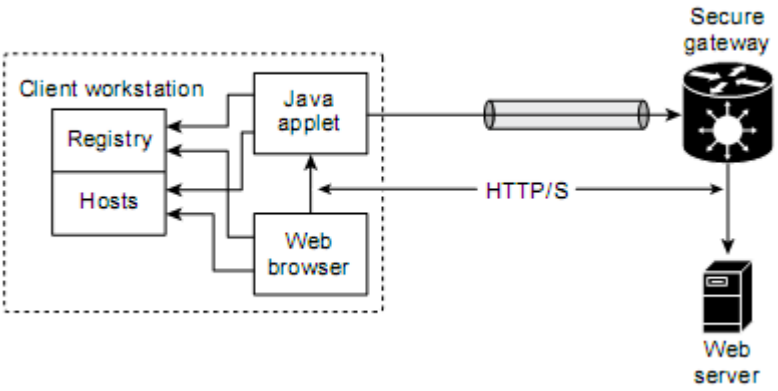
1) Clientless

V tomto režimu vzdálený uživatel přistupuje do interní (např. firemní) sítě použitím internetového prohlížeče na klientském počítači (viz obr.1 A). V tomto módu jsou dostupné tyto aplikace:

- Internetové prohlížení (používající HTTP a zabezpečené HTTPS) – portálová stránka poskytuje seznam URL webových serverů, které může vzdálený uživatel prohlížet
- Sdílení souborů (používající společný souborový systém [CIFS]) – portálová stránka poskytuje seznam souborových serverů, kde může vzdálený uživatel provádět tyto operace:
    - prohlížení sdílených souborů
    - vytváření souborů/adresářů
    - přejmenování adresářů
    - nahrání/stažení souborů
    - přejmenování/smazání souborů

2) Thin-Client

Tento způsob se nazývaná přesměrování portu. Předpokládá, že klientská aplikace použije TCP spojení na známý server a port. Vzdálený uživatel si stáhne Java applet kliknutím na odkaz na portálové stránce, nebo je stažen automaticky. Java applet funguje na klientovi jako TCP proxy pro služby, které jsou nakonfigurovány na portálové stránce (viz obr.1 B). Tento typ rozšiřuje šifrovací schopnosti webového prohlížeče a umožňuje vzdálený přístup k aplikacím založeným na TCP jako jsou POP3, SMTP, IMAP, telnet a SSH.



Obr.2 Thin-client

Obrázek 2 ukazuje komunikaci klientské stanice skrz zabezpečenou bránou. Veškerá komunikace s gateway je zajištěna přes java applet. Java applet hraje roli proxy serveru. Veškeré požadavky jsou nejdříve zaslány na applet a ten pak otevře spojení na zabezpečenou bránu a odešle požadavky z prohlížeče. Ukládá si nastavení proxy konfigurace z webového prohlížeče. Před uzavřením applet zruší uložené konfigurace.

Požadavky: - klient musí mít povoleno stahování a instalování Java appletů

3) Tunnel

V tomto módu má vzdálený uživatel největší možnosti. Nabízí rozsáhlejší podporu aplikací přes dynamicky stáhnutelný Cisco AnyConnect VPN klienta pro SSL VPN. Klient poskytuje virtuální přístup k síťové vrstvě různým aplikacím. Tento typ poskytuje přístup ke stále zvětšující se množině běžně dostupných aplikací jako je prohlížení stránek, služby přes web (přistup k souborům), e-mail a aplikace založené na TCP. Přináší dostupnost mnoha internetových aplikací bez nutnosti jejich instalace na klientské stanici

Tunelové spojení se navazuje na základě skupinové politiky. Např. Cisco AnyConnect VPN klient je stáhnut a nainstalován na klientský počítač (obr.1 C). Spojení je navázáno po přihlášení vzdáleného uživatele na SSL VPN bráně. Po ukončení spojení se Cisco AnyConnect VPN klient odstraní z klientské stanice (nebo může zůstat na stanici nainstalován).

Tabulka shrnující jednotlivé módy

Clientless	Thin klient	Tunnel
založen na prohlížeči	TCP přesměrování portu	"clientless" IPSec VPN
Webové aplikace, sdílení	používá Java applet	používá Java nebo ActiveX
brána poskytuje obsah	Telnet, email, SSH aplikace založené na statickém portu	použitelné pro všechny aplikace založené na IP

Obecné požadavky pro SSL VPN

- Zřízený uživatelský účet
- Podpora SSL v internetovém prohlížeči
- Podporu OS (MS Windows 2000, Mac OS X, Linux Fedora 5, …)
- Webový prohlížeč s podporou SSL VPN (IE 6, Firefox 2 a Safari 2.0.3)

Konfigurace SSL VPN

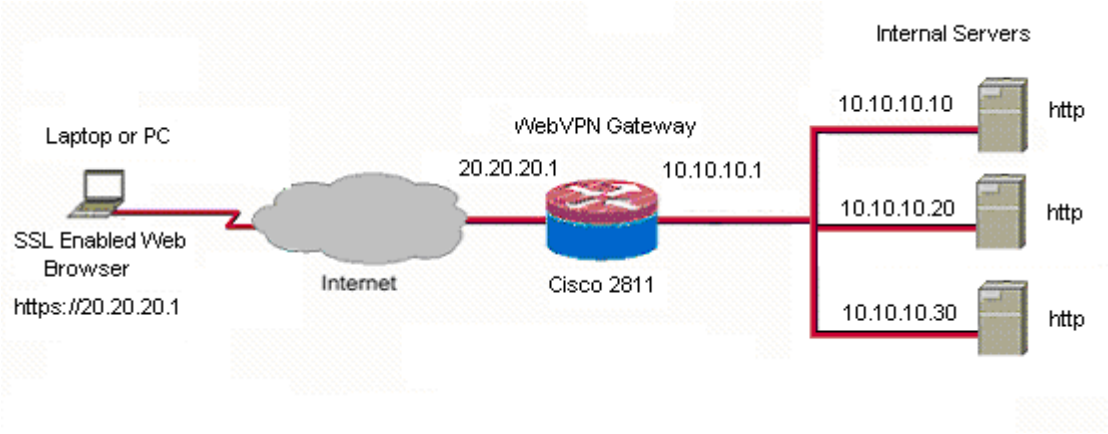
V této části popisujeme konfiguraci SSL VPN. První případ je nakonfigurování a otestování typu Clientless SSL VPN a v druhém případě konfigurace a otestování typu Thin-client SSL VPN. Vybrané řešení jsme odzkoušeli na Cisco routeru 2811 s IOS 12.4.9.

I. Konfigurace Clientless

Kroky vedoucí k úspěšné konfiguraci jsou následující:

- Konfigurace WebVPN Gateway – brána do privátní sítě
- Konfigurace WebVPN Policy Group a výběrů zdrojů
  - Group policy specifikuje charakteristickou vlastnost a parametry (autentizace, autorizace), které mohou být využívaný pro každou SSL VPN virtuální instanci. Vlastnosti mohou být povolovány nebo zakázány práve v group policy, která je spojena s SSL VPN kontextem
- Konfigurace WebVPN kontextu
  - Kontext obsahuje všechny prvky group policy, které mohou být využity na uživatele jako např. autorizace, autentizace atd, Využívá Webvpn gateway.

Topologie řešení



Jednotlivé příkazy pro směrovač

Nastavení interface na Cisco 2811:

```
interface FastEthernet 0/0
 ip address 10.10.10.1 255.255.255.0        //za tímto interface se skrývá vnitřní síť
 no sh
exit
```

```
interface FastEthernet 0/1
 ip address 20.20.20.1 255.255.255.0        //za tímto interface se skrývá vnější síť
 no sh
exit
```

Zapnutí AAA autentifikace - konfigurace lokální databáze:

```
aaa new-model                               // povolení aaa globálně

aaa authentication login default local      // vytvoří autentizační lokální list

aaa authorization exec default local        //

exit
```

Vytvoření certifikátu:

Pomocí certifikátu se vytvoří přístupový bod, kterému můžeme důvěřovat při přihlašování přes SSL VPN.

```
crypto ca trustpoint Router_Certificate
```

//K identifikaci důvěrného bodu (truspoint), který je využíván k validaci certifikátu během výměny klíčů IKE autentizace.

```
 rsakeypair Router_Certificate 512
```

//Ke specifikaci, který pár klíčů je spojený s certifikátem.

```
 ip-address none

 enrollment selfsigned
```

//Specifikuje sám sebou podepsané přihlášení k bezpečnému bodu (truspoint).

```
 serial-number none

 exit
```

Vytvoření SSL VPN gateway:

```
webvpn gateway GATEWAY          //vytvoření Gateway

 ip address 20.20.20.1 port 443 //Gateway je specifikována na adrese 20.20.20.1

 hostname cisco2800             // název hostitele Cisco2800

 http-redirect port 80          // přesměrování na HTTP

 inservice

 ssl trustpoint Router_Certificate  // delkarace důvěryhodného bodu v záštitě certifikátu
```

```
 exit
```

Povolení zdrojů:

```
webvpn context Context1                 // vytvoření wevpn contextu Context
 gateway Gateway                        // přiřazení gateway pod názvem Gateway do kontextu
 inservice
 max-users 2                            // maximální počet uživatelů 2
 nbns-list NBNS         // deklarace NetBIOS Name Service, předává SSL VPN kontext
  nbns-server 10.10.10.30 master
  exit
 url-list "Servers"      //vytvoření zdrojů kam může přihlášený uživatel jít pod listem Server
  url-text "Server1" url-value http://10.10.10.10     //povolení vnitřního zdroje
  url-text "Server2" url-value http://10.10.10.20     //povolení vnitřního zdroje
  heading "Servers"
  exit
```

Policy group

```
 policy group policy1             // deklarace policy group pod jménem policy1
  functions file-access
  functions file-entry
  functions file-browse
  nbns-list NBNS                  // NBNS musí být definován v Group policy
  url-list Servers                // povolení listu Servers na portál stránce
  exit
 default-group-policy policy1  // přiřazení politiky
 exit
```

Přidání uživatele (přidáme dva uživatele, kteří se mohou přihlásit k SSL VPN bráně)

```
username jenik secret jenik0          //vytvoření uživatele jenik
username petr secret petr00           //vytvoření uživatele petr
```

Stav SSL VPN na routeru

Router#show webvpn gateway

Zobrazuje stav gateway. Hodnota up znamená zapnutá funkce. Viz. Rozšíření verze níže.

Gateway Name Admin Operation

---------- ----- ---------

gateway_1 up up

Router#show webvpn context

Zobrazuje stav a parametry SSL VPN kontextu. Parametry Contextname je jméno kontextu. Gateway je jméno asociované gateway. VRF zobrazuje VPN routování a forwardování. AS administrativní stav. OS operativní stav.

Context Name Gateway Domain/VHost VRF AS OS

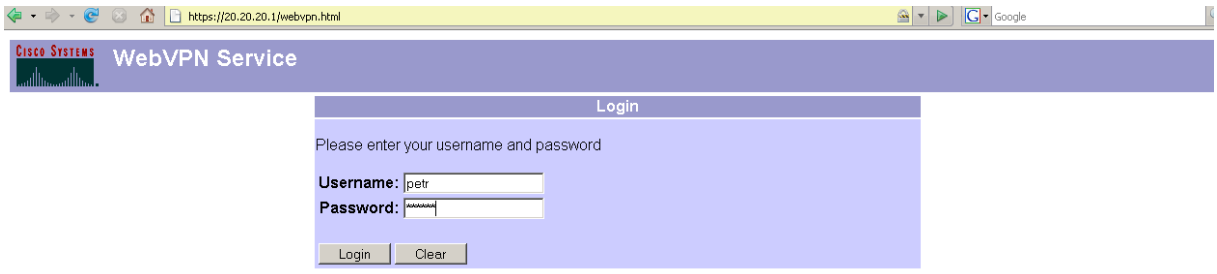
---------- ------- ---------- ------- ---- --------

webvpn gateway_1 - - up up

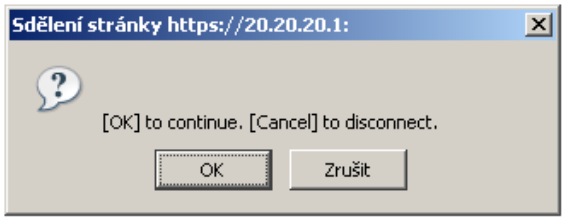
Ověření funkčnosti

V této části jsou zobrazeny sejmuté obrazovky z klientského počítače pro ověření správné konfigurace.

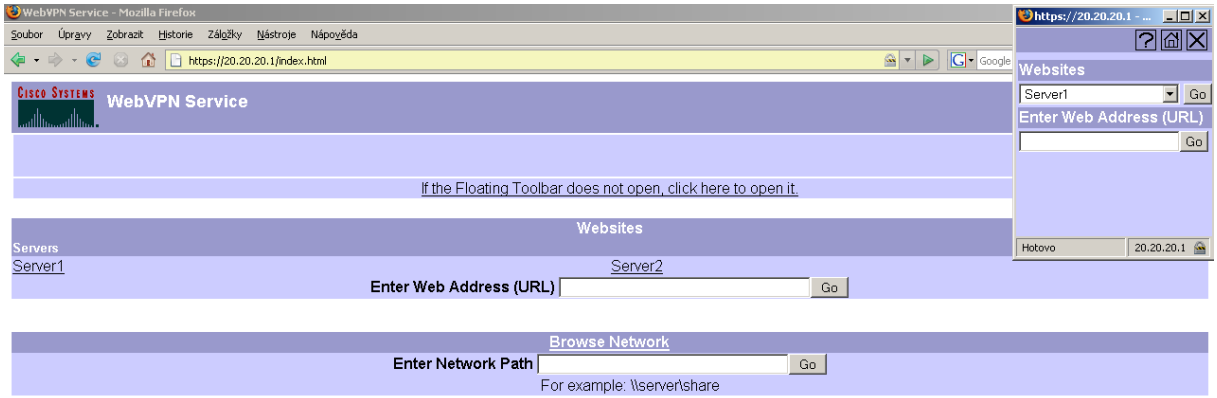
Postup ověření přístupu je:
- spuštění www prohlížeče a zadání adresy brány
- přihlášení uživatele pomocí jména a hesla (obr.3)
- zobrazí se okno, zda chceme pokračovat v přihlášení (obr.4)
- zobrazení dostupných serverů pro přihlášeného uživatele (obr.5)
- připojení na vybraný server (obr.6)
- pokus o připojení na vybraný sdílený zdroj (obr.7)
- odhlášení uživatele (obr.8)



Obr.3 Úvodní obrazovka

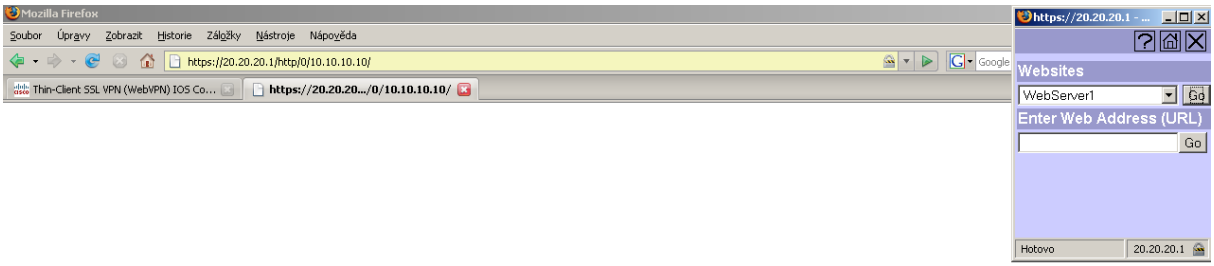


Obr.4 Úspěšné přihlášení



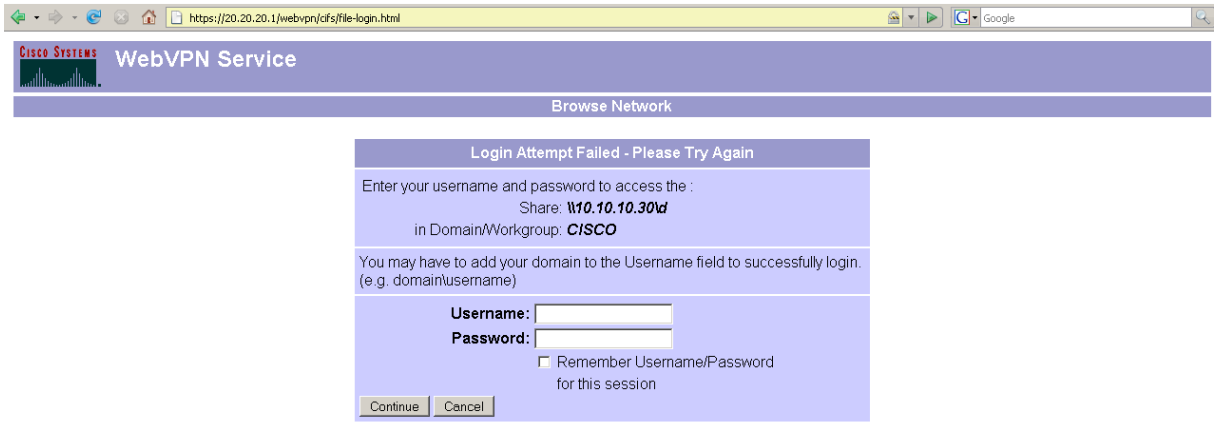
Obr.5 Seznam dostupných serverů

Na obrázku 5 je zobrazena stránka SSL VPN brány s dostupnými servery (zde Server1 a Server2) v prostřední části obrazovky a dolní části pole pro zadání adresy. Navíc je zobrazeno nové menší okno s výběrem serverů z roletové nabídky a možnosti zadání adresy serveru (pokud bychom se chtěli dostat na server, který není uvedený v nabídce).



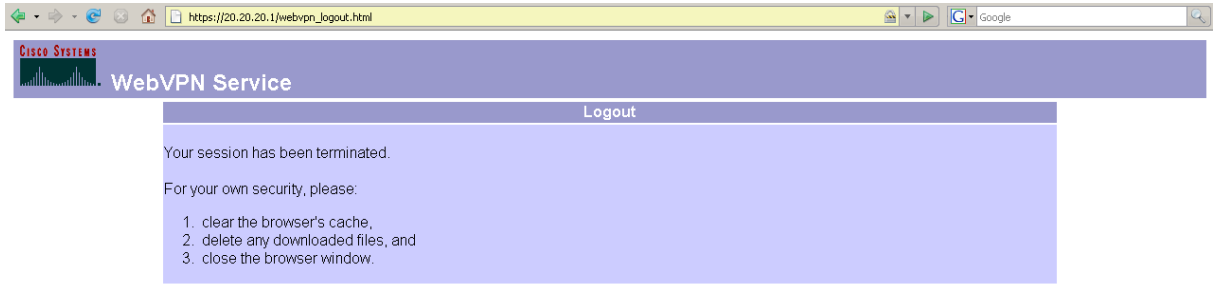
Obr.6 Připojení na vybraný server

Obrázek 6 ukazuje úspěšné připojení na server WebServer1.



Obr.7 Pokus o připojení na sdílený zdroj

Obrázek 7 zobrazuje okno pro přihlášení na sdílený zdroj v interní síti. Přihlášení se nám nepodařilo uskutečnit. Bohužel jsme nebyli schopni se připojit se správným jménem a heslem. To zřejmě způsobilo nepsrávné nastavení sdíleného zdroje.

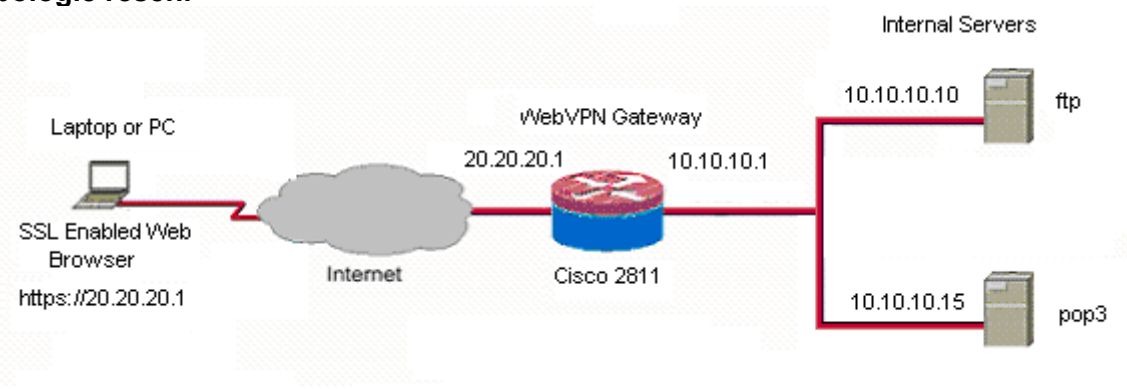


Obr.8 Odhlášení

Konfigurace Thin-client

Kroky jsou velice podobné jako u typu clientless. Rozdíl je v definování dostupných zdrojů a bezpečnostní politiky policy group.

Topologie řešení



Jednotlivé příkazy pro směrovač

Nastavení interface na Cisco 2811:

```
interface FastEthernet 0/0
 ip address 10.10.10.1 255.255.255.0        //za tímto interface se skrývá vnitřní síť
 no sh
exit

interface FastEthernet 0/1
 ip address 20.20.20.1 255.255.255.0        //za tímto interface se skrývá vnější síť
 no sh
exit
```

Zapnutí AAA autentifikace - konfigurace lokální databáze:

```
Aaa new-model                               // povolení aaa globálně

aaa authentication login sdm_vpn local      // vytvoření lokálního autentizačního listu
```

Vytvoření certifikátu:

Pomocí certifikátu se vytvoří přístupový bod, kterému můžeme důvěřovat při přihlašování přes SSL VPN.

```
crypto ca trustpoint Router_Certificate
```

//K identifikaci důvěrného bodu (truspoint), který je využíván k validaci certifikátu během výměny klíčů IKE autentizace.

rsakeypair Router_Certificate 512

//Ke specifikaci, který pár klíčů je spojený s certifikátem.

ip-address none

enrollment selfsigned

//Specifikuje sám sebou podepsané přihlášení k bezpečnému bodu (truspoint).

serial-number none

exit

Vytvoření gateway:

webvpn gateway gateway_1	//deklarace Gateway s názvem gateway_1
ip address 20.20.20.1 port 443	// Gatewy je deklarována na adrese 20.20.20.1
http-redirect port 80	// přesměrování na HTTP
inservice	
ssl trustpoint Router_Certificate	// delkarace důvěryhodného bodu v záštitě certifikátu
exit	

Konfigurace kontextu

webvpn context webvpn	// deklarace contextu webvpn
aaa authentication list sdm_vpn	
gateway gateway_1	// vložení Gateway gateway_1 do kontextu
inservice	
max-users 1000	// max počet uživatelů 1000
secondary-color white	// jak bude vypadat stránka kontextu
title-color #CCCC66	
text-color black	
policy group policy_1	// vložení policy group s názvem policy_1 do kontextu
exit	
default-group-policy policy_1	// deklarace default group policy max vždy jedna
exit	

Konfigurace zdrojů

```
webvpn context webvpn                  // konfigurace zdrojů pro kontext
 port-forward portforward_list_1       // vytvoření listu zdrojů
  local-port 3001 remote-server 10.10.10.15 remote-port 110 description "POP3 Server"
  // vytvoření vzdáleného zdroje POP3 s adresou vnitřní sítě 10.10.10.15
  local-port 3000 remote-server 10.10.10.10 remote-port 21 description "FTP server"
  // vytvoření vzdáleného zdroje FTP s adresou vnitřní sítě 10.10.10.10
exit
```

Policy group

```
 policy group policy_1
  port-forward portforward_list_1      // přidání listu zdrojů do policy group s názvem policy_1
  exit
 exit
```

Přidání uživatele (přidáme dva uživatele, kteří se mohou přihlásit k SSL VPN bráně)

```
username jenik secret jenik0          //vytvoření uživatele jenik
username petr secret petr00           //vytvoření uživatele petr
```

Stav SSL VPN na routeru

```
Router#show webvpn stats

User session statistics:
```

Active user sessions	: 2	AAA pending reqs	: 0
Peak user sessions	: 2	Peak time	: 00:00:28
Active user TCP conns	: 3	Terminated user sessions	: 0
Processed req hdr bytes	: 36142	Processed req body bytes	: 94
HTTP/1.0 responses	: 0	HTTP/1.1 responses	: 0

Active user session - počet přihlášených uživatelů, Active user TCP conn – počet TCP, které využívá uživatel, Processed req hdr bytes – počet zpracovaných hlaviček žádostí, Peak time doba připojení uživatele, Processed req body bytes – počet zpracovaných žádostí.

```
Router#show webvpn gateway
```

Popsáno viz. výše (clientless)

Gateway Name Admin Operation

gateway_1 up up

Router#show webvpn context

Popsáno viz. výše (clientless)

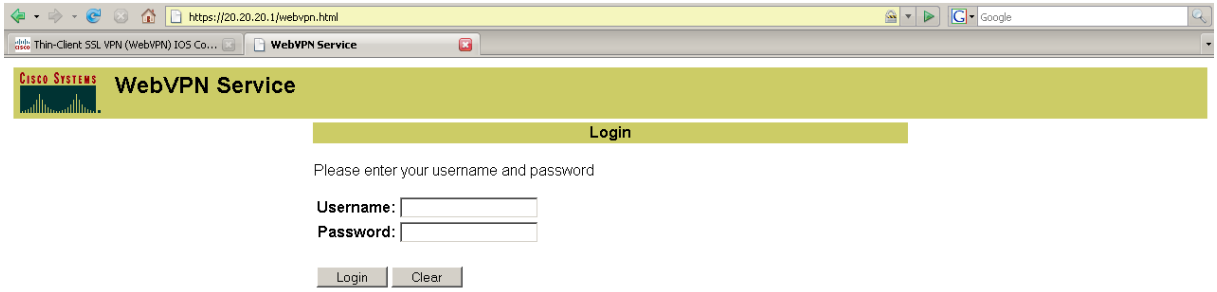
Context Name Gateway Domain/VHost VRF AS OS

webvpn gateway_1 - - up up

Ověření funkčnosti

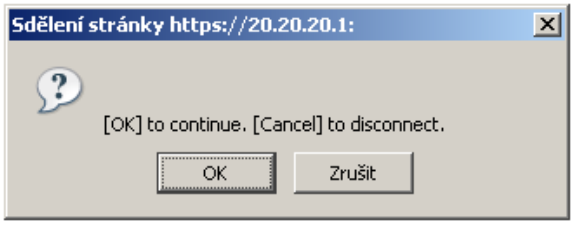
V této části jsou zobrazeny sejmuté obrazovky z klientského počítače pro ověření správné konfigurace.

Postup ověření přístupu je:
- spuštění www prohlížeče a zadání adresy brány (obr.9)
- přihlášení uživatele pomocí jména a hesla
- zobrazí se okno, zda chceme pokračovat v přihlášení (obr.10)
- zobrazení stránky SSL VPN brány (obr.11)
- zobrazení dostupných serverů pro uživatele (obr.12+13)

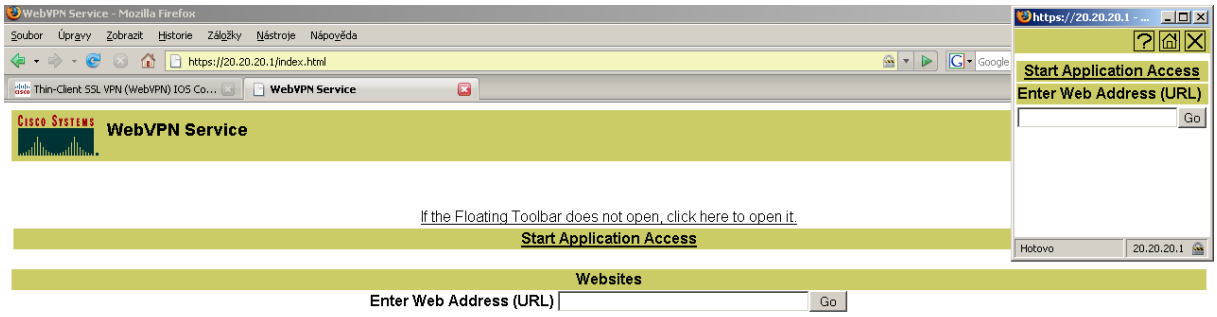


Obr.9 Připojení na bránu

Vyplněním správného jména a hesla se uživatel úspěšně připojí na SSL VPN bránu.

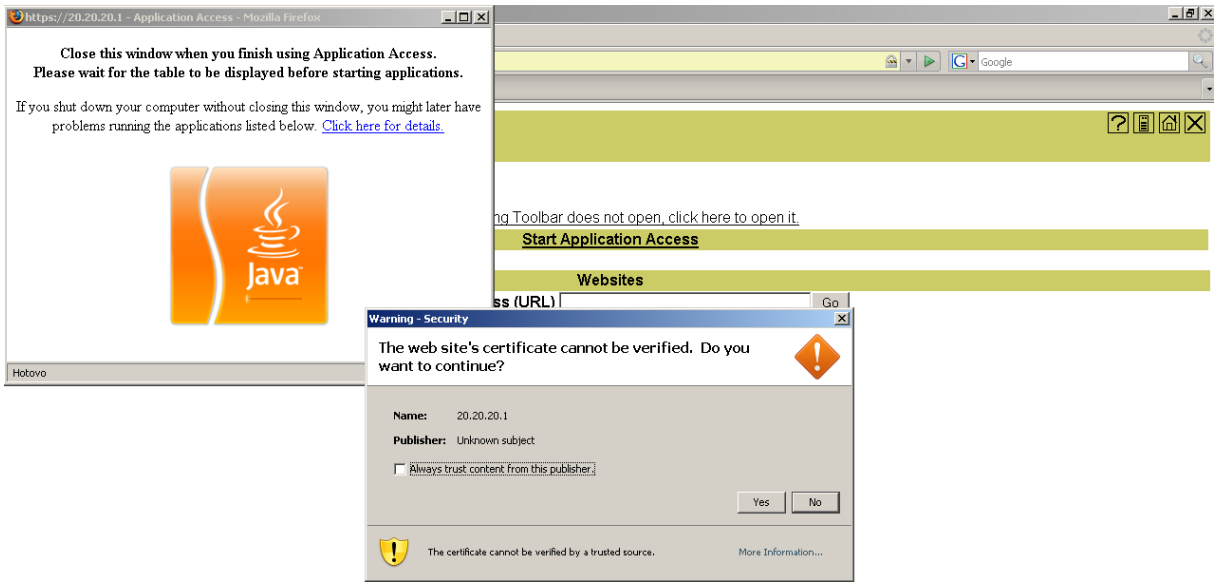


Obr.10 Uživatel přihlášen

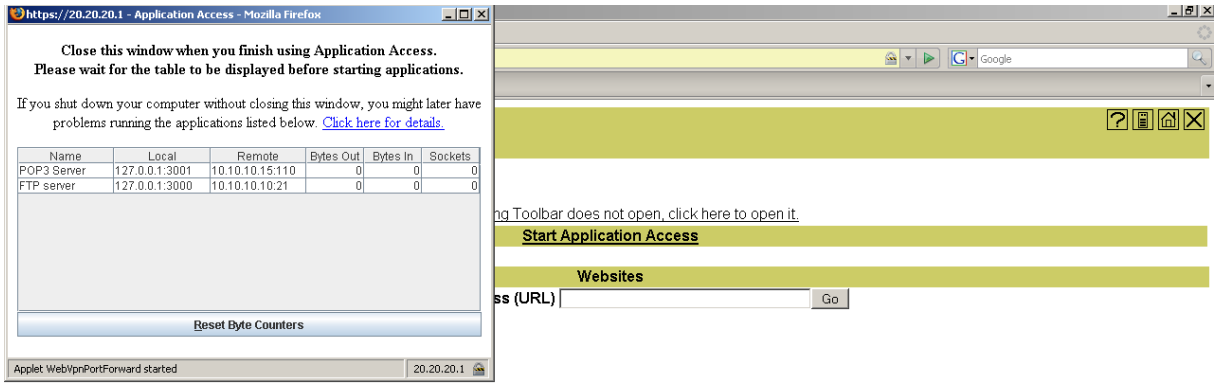


Obr.11 Stránka brány

Obrázek 11 ukazuje hlavní stránku SSL VPN brány (uživateli se navíc zobrazí malé okno), kde uživatel může vyplnit URL adresu a tlačítkem GO přejít na server (pokud existuje v interní síti), nebo kliknutím na Start Application Access je uživateli zobrazena tabulka dostupných serverů (obr.13). Před zobrazením je po potvrzení stáhnut appletu (obr.12).



Obr.12 Stáhnutí appletu



Obr.13 Seznam dostupných serverů

Závěr

V této práci jsme nakonfigurovali a otestovali dva módy SSL VPN připojení ve školní laboratoři. Jednalo se o Clientless a Thin-client řešení. Obě řešení fungovala bez problémů. Abychom mohli potvrdit funkci všeobecně v počítačových sítích, museli bychom vyzkoušet složitější topologii s větším množstvím jak serverů v interní sítí, tak více přistupujících klientů, což není v našich podmínkách možné.