KAPITOLA 10

Zabezpečení

Mezi témata zkoušky CCNA probíraná v této kapitole patří:

- **Identifikace bezpečnostních hrozeb sítě a popis obecných metod, jak tyto hrozby zmírnit**
  - Popis současné situace s nárůstem síťových hrozeb a vysvětlení toho, proč je kvůli zmírnění hrozeb potřebné implementovat komplexní zásady zabezpečení
  - Vysvětlení obecných metod zmírnění běžných bezpečnostních hrozeb, které se týkají síťových zařízení, hostitelů a aplikací
  - Popis fungování běžných bezpečnostních zařízení a aplikací
  - Popis doporučených zásad zabezpečení včetně počátečních kroků při zabezpečení síťových zařízení
- **Konfigurace, kontrola a řešení potíží základních funkcí směrovače a směrování se zařízeními Cisco**
  - Implementace základního zabezpečení směrovače
- **Implementace, kontrola a řešení potíží s překladem adres NAT a seznamy ACL ve středně velké síti v podnikové pobočce**
  - Popis účelu a typů seznamů ACL
  - Konfigurace a použití seznamů ACL na základě požadavků filtrování sítě (včetně rozhraní příkazového řádku a nástroje SDM)

- Konfigurace a použití seznamů ACL při omezení přístupu ke směrovači pomocí protokolů telnet a SSH (včetně nástroje SDM a rozhraní příkazového řádku)
- Kontrola a sledování seznamů ACL v síťovém prostředí
- Řešení potíží se seznamy ACL

Jistě budete souhlasit, že hlavní prioritou správce sítě by měla být ochrana citlivých a kritických dat spolu se síťovými prostředky před všemi druhy zneužití. Jste na správné straně – společnost Cisco nabízí skutečně efektivní bezpečnostní řešení, která k tomu poskytují potřebné nástroje.

V této kapitole se zaměříme hlavně na to, jak chránit uživatele a interní síť. Hodně místa věnujeme prevenci nejčastějších hrozeb zabezpečení sítě pomocí směrovačů Cisco a firewallů se systémem IOS, které společně poskytují velmi výkonné integrované řešení na ochranu před mnoha typy průniků. Uvedeme základní fakta o tom, jak Cisco IOS Firewall poskytuje zabezpečení a vynucení zásad vzhledem k požadavkům interní a externí sítě. Ukážeme si také, jak navázat zabezpečená připojení k libovolným vzdáleným umístěním.

Přístupové seznamy (ACL – access control list) jsou integrální součástí bezpečnostních řešení Cisco. Příklady jednoduchých i pokročilých přístupových seznamů v této kapitole umožní zajistit bezpečnost datové sítě i minimalizovat většinu rizik pro bezpečnost sítě.

Správné použití a konfigurace přístupových seznamů představuje důležitou součást konfigurace směrovačů, protože tyto seznamy patří mezi velice pružné síťové nástroje. Přístupové seznamy zásadně přispívají k efektivitě a funkčnosti sítě. Správcům pak poskytují mimořádnou úroveň kontroly nad tokem dat v rámci podniku. U přístupových seznamů mohou správci shromažďovat základní statistiky toku paketů a implementovat zásady zabezpečení. Lze také chránit citlivá zařízení před neautorizovaným přístupem.

V této kapitole rozebereme přístupové seznamy protokolu TCP/IP a MAC adres u přepínače vrstvy 2 a zmíníme se také o některých nástrojích, které jsou k dispozici při testování a sledování funkčnosti aplikovaných přístupových seznamů.

Jakmile popíšeme Cisco IOS Firewall a konfiguraci přístupových seznamů pomocí rozhraní příkazového řádku, ukážeme si, jak konfiguraci usnadňuje nástroj Cisco SDM (Security Device Manager).

Sítě VPN (virtual private network) sice mohou tvořit důležitou součást podnikové bezpečnosti, ale těmito sítěmi se budeme zabývat až v kapitole 14, „Rozlehlé sítě WAN“.

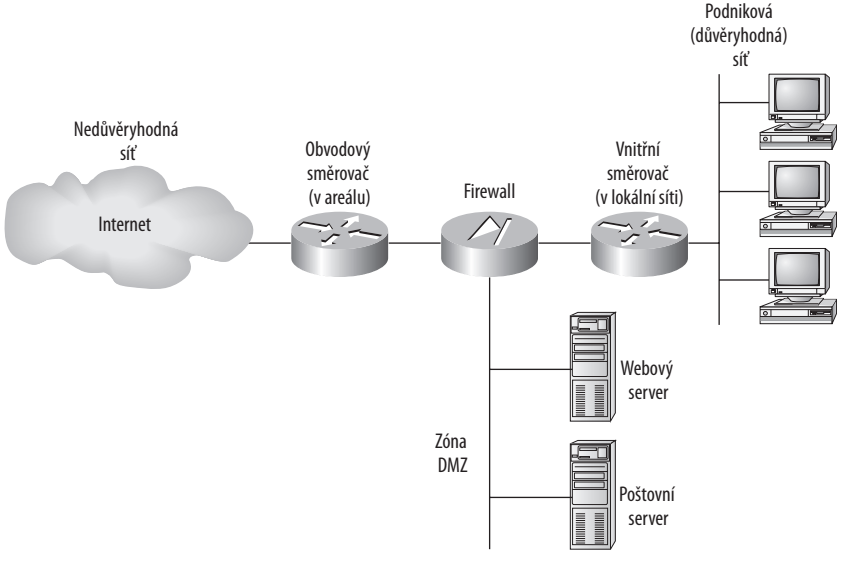
Poznámka

Nejčerstvější aktualizace této kapitoly naleznete na adrese `www.lammle.com` **nebo** `www.sybex.com`.

Obvodové, firewallové a vnitřní směrovače

Často se setkáte s tím, že ve středních až velkých podnikových sítích jsou různé bezpečnostní strategie založeny na určité kombinaci vnitřních a obvodových směrovačů spolu s firewally.

Vnitřní směrovače poskytují další úroveň zabezpečení sítě, protože monitorují provoz do různých částí chráněné podnikové sítě na základě přístupových seznamů. Umístění jednotlivých typů těchto zařízení znázorňuje obrázek 10.1.



Obrázek 10.1: Typická zabezpečená síť

V této kapitole a kapitole 11, „Překlady adres NAT (Network Address Translation)", budeme často používat termíny *důvěryhodná síť* a *nedůvěryhodná síť*. Proto byste měli vědět, kde se tyto části v typické zabezpečené síti nacházejí. Zóna DMZ (demilitarized zone) může v závislosti na konfiguraci firewallu používat globální (skutečné) internetové adresy nebo privátní adresy, ale obvykle zahrnuje servery HTTP, DNS, poštovní servery a další podnikové servery poskytující služby internetového typu.

Jak již víte, lze místo směrovačů nastavit ve vnitřní důvěryhodné síti sítě VLAN (virtual local area network) s přepínači. Přepínače pro více vrstev vybavené vlastními bezpečnostními funkcemi mohou někdy nahradit vnitřní směrovače (sítě LAN) a zvýšit výkon architektury se sítěmi VLAN.

Rozeberme nyní bezpečnostní rizika, která hrozí v typické zabezpečené datové síti. Poté si ukážeme několik způsobů ochrany datové sítě pomocí sady funkcí Cisco IOS Firewall a přístupových seznamů.

Jaké známe bezpečnostní hrozby

Ano, je to tak: Bezpečnostní útoky se značně liší svou složitostí a závažností hrozby. K některým z nich dokonce dochází kvůli HUI neboli hloupé uživatelské ignoranci. (Tento termín sice v okruzích zkoušky nenajdete, ale uplatňuje se častěji, než byste čekali!)

Všechno se v posledku odvíjí od plánování nebo jeho nedostatku. Internet, který dnes zastává nezastupitelnou roli, se vyvinul způsobem, jaký jeho tvůrci absolutně nepředpokládali. To je základní důvod, proč nyní máme takové problémy s bezpečností – většina implementací protokolu IP je z podstaty nezabezpečená. Není však třeba se bát, protože společnost Cisco nabízí několik triků, jak všechny potíže vyřešit. Nejdříve však prozkoumejme některé běžné typy útoků:

Útoky na aplikační vrstvě – tyto útoky se běžně soustřeďují na známé bezpečnostní díry softwaru, který obvykle funguje na serverech. K oblíbeným cílům patří FTP, sendmail a HTTP. Vzhledem k tomu, že příslušné účty mají nejčastěji „privilegovaná" oprávnění, mohou útočníci jednoduše získat přístup a zneužít počítač, kde jsou uvedené aplikace spuštěny.

„Autorooters" – můžete si je představit jako hackerské roboty. Hackeři často pomocí tzv. rootkitu testují, skenují a poté zachytávají data v strategicky umístěném počítači, který jim poskytuje „oči" do celé sítě, a to automaticky!

Zadní vrátka – jedná se prostě o cesty, které vedou do počítače nebo sítě. Pomocí jednoduchých průniků nebo komplikovanějšího kódu „trojských koní" mohou hackeři použít implantované trasy ke konkrétnímu hostiteli nebo dokonce síti kdykoli chtějí – samozřejmě dokud je neodhalíte a nezastavíte!

Útoky DoS (denial of service) a DDoS (distributed denial of service) – tyto útoky jsou závažné a velmi těžko se před nimi brání. Avšak ani hackeři nemají respekt před svými kolegy, kteří tyto útoky spouštějí. Ačkoli jsou nepříjemné, dají se provést poměrně snadno. (To znamená, že vaši síť může položit nějaké desetileté dítě, což není příliš fér.) Princip je založen na zahlcení systému, který normálně poskytuje určitou službu. Existuje několik různých variant tohoto typu útoků:

> **Záplava TCP SYN** – klient nejdříve inicializuje zdánlivě běžné připojení protokolu TCP a odešle serveru zprávu SYN. Server odpoví očekávaným způsobem a odešle zprávu SYN-ACK zpět klientskému počítači, který poté naváže spojení tím, že vrátí zprávu ACK. To vypadá bezproblémově, ale ve skutečnosti je během tohoto procesu – kdy je připojení otevřeno pouze napůl – napadený počítač doslova zaplaven napůl otevřenými připojeními a prakticky je vyřazen z provozu.
>
> **Útoky typu „ping of death"** – pravděpodobně víte, že pakety protokolu TCP/IP mají maximální velikost 65 536 oktetů. Pokud to náhodou nevíte, nic se neděje. Měli byste však rozumět tomu, že při tomto útoku se jednoduše odesílají příliš velké pakety příkazu ping. Cílové zařízení se tak neustále restartuje, zamrzá nebo úplně havaruje.
>
> **TFN (Tribe Flood Network) a TFN2K (Tribe Flood Network 2000)** – tyto nemilé malé triky jsou složitější, protože inicializují synchronizované útoky DoS z více zdrojů a mohou být zaměřeny na více zařízení. Na jejich úspěchu se zčásti podílí tzv. „falšování IP", které si brzy vysvětlíme.

Stacheldraht – tento útok je v praxi kombinací metod a jeho název znamená v němčině „ostnatý drát". V zásadě je založen na útoku TFN doplněném o šifrování. Začíná mohutnou invazí na kořenové úrovni, po které následuje závěrečný útok typu DoS.

Falšování IP – princip tohoto útoku je zřejmý z jeho názvu – útočník uvnitř nebo vně sítě se maskuje jako důvěryhodný hostitelský počítač. Přitom používá jeden z těchto dvou postupů: Předloží IP adresu v rámci rozsahu důvěryhodných síťových adres, nebo použije schválenou a důvěryhodnou externí IP adresu. Vzhledem k tomu, že skutečná identita hackera se ukrývá za falšovanou adresou, často tím skutečné problémy teprve začínají.

Útoky prostředníka – tyto útoky zachytávají cenné síťové pakety. Viník často pracuje u poskytovatele internetových služeb a používá nástroj označovaný jako sledovací program (sniffer – viz dále) a aplikuje jej na směrovací a transportní protokoly.

Průzkum sítě – před nabouráním do sítě o ní hackeři často shromažďují veškeré dostupné informace, protože čím více toho o síti vědí, tím lépe ji dokáží narušit. Ke svým cílům využívají metody typu skenování portů, dotazů DNS a hromadných příkazů ping.

Sledování paketů – tento nástroj jsme již zmínili výše, ale neuvedli jsme jeho princip. Možná překvapivě se ve skutečnosti jedná o software. Funguje takto: karta síťového adaptéru je nastavena do promiskuitního režimu, takže všechny pakety zachycené na fyzické vrstvě sítě odesílá speciální aplikaci, která je třídí a analyzuje. Nástroj pro sledování paketů může odposlechnout některá vysoce cenná a citlivá data včetně hesel a uživatelských jmen. Tyto nástroje jsou proto velmi oblíbené u útočníků, kteří chtějí zcizit cizí identitu.

Útoky na hesla – tyto útoky mají mnoho podob a i když je lze realizovat mnoha sofistikovanými metodami typu falšování IP, sledování paketů a trojských koní, je jejich jediným účelem (překvapivě) zjištění uživatelských hesel, aby se mohl zloděj vydávat za oprávněného uživatele a využívat jeho privilegia a prostředky.

Útok hrubou silou – další softwarově orientovaný útok využívá program spuštěný v cílové síti, který se pokouší přihlásit k některému typu sdíleného síťového prostředku, jako je server. Pro hackera je ideální, pokud má napadený účet dostatečná oprávnění, protože poté může vytvořit zadní vrátka pro pozdější přístup a nutnost zadávání hesel úplně obejít.

Útoky s přesměrováním portu – tento přístup vyžaduje, aby se hacker úspěšně dostal do hostitelského počítače. Umožňuje přenášet přes firewall podezřelý provoz (který by byl normálně zakázán).

Útoky trojských koní a virů – tyto dva vektory jsou v zásadě velmi podobné. Jak trojské koně, tak viry infikují počítače uživatelů škodlivým kódem a do různé míry manipulují s paralýzou, ničením nebo dokonce likvidací! Jsou však mezi nimi určité rozdíly – viry jsou skutečně pouze nepříjemné programy připojené ke kódu command.com, což je náhodou hlavní příkazový interpret všech systémů Windows. Viry poté divoce odstraňují soubory a infikují všechny varianty souboru command.com, které mohou v nakaženém počítači najít. Rozdíl mezi viry a trojskými koni spočívá v tom, že trojské koně jsou v praxi kompletní aplikace vložené do kódu, díky kterému vypadají jako zcela odlišná entita. Tyto ničivé nástroje se například maskují jako jednoduchá neškodná hra!

Útoky se zneužitím důvěryhodnosti – dochází k nim, když někdo zneužije vztah důvěryhodnosti v rámci lokální sítě. Obvod podnikové sítě například často zahrnuje důležité počíta-

če typu serverů SMTP, DNS a HTTP. Tyto servery jsou kvůli tomu značně zranitelné, protože se nacházejí ve stejném segmentu.

Po pravdě řečeno se nebudeme pouštět do podrobností ohledně toho, jak jednotlivé právě zmíněné hrozby zmírnit. To by totiž jednak přesahovalo rozsah této knihy, ale navíc metody, které si ukážeme, fungují jako účinná obecná prevence útoků. Naučíte se tolik triků, že dokážete odradit všechny útočníky s výjimkou těch nejodhodlanějších. V zásadě tedy v této kapitole najdete rady týkající se „zabezpečení sítí".

Jak potlačit bezpečnostní hrozby

Jaké řešení je při prevenci bezpečnostních hrozeb vhodné? Něco od firmy Juniper, McAfee, nebo snad jiný produkt typu firewall? Ale ne – nejspíš bychom měli zvolit něco od společnosti Cisco. Cisco nabízí velmi zajímavý produkt s názvem ASA neboli Adaptive Security Appliance. Má to však jeden nebo dva háčky – tento malý zázrak je poměrně drahý a jeho cena roste v závislosti na vybraných modulech (například prevence průniku). Nástroj ASA navíc přesahuje rámec cílů této knihy. Podle autora této knihy se jedná o nejlepší produkt na trhu.

Software Cisco IOS funguje na více než 80 procentech páteřních směrovačů Internetu a pravděpodobně se jedná o nejkritičtější část síťové infrastruktury. Zůstaňme tedy při zemi a v rámci každodenních potřeb bezpečnosti internetového připojení, intranetu a vzdáleného přístupu použijme softwarové zabezpečení systému Cisco IOS, které se označuje jako sada funkcí Cisco IOS Firewall. Tento přístup je určitě rozumný, protože přístupové seznamy Cisco skutečně účinně chrání před mnohými běžnými bezpečnostními hrozbami. Pokud se navíc náhodou připravujete na zkoušku CCNA, je znalost fungování přístupových seznamů nejdůležitějším tématem této kapitoly!

Cisco IOS Firewall

Následuje seznam možností, díky kterým Cisco IOS Firewall zmírňuje některé běžné bezpečnostní hrozby:

Modul stavové kontroly IOS Firewall – jedná se o funkci ochrany obvodu sítě, protože poskytuje interním uživatelům bezpečnou kontrolu přístupu v závislosti na aplikaci. Často se označuje jako CBAC (ContextBased Access Control).

Detekce průniku – nástroj podrobné kontroly paketů, které dovoluje sledovat, zachycovat a reagovat na napadení v reálném čase, protože rozpoznává 102 nejčastějších charakteristik útoků a průniků.

Přenos hlasu přes firewall – funkce na aplikační úrovni, která je založena na znalosti toku volání protokolu a také relevantních otevřených kanálech. Podporuje hlasové protokoly H.323v2 a SIP (Session Initiation Protocol).

Kontrola ICMP – v zásadě povoluje reakce na pakety ICMP jako ping a traceroute, které pocházejí z vnitřní strany firewallu, zatímco zahazuje jiný provoz protokolu ICMP.

Autentizační proxy – nová funkce, která uživatelům kdykoli umožňuje autentizaci přístupu k síťovým prostředkům pomocí protokolů HTTP, HTTPS, FTP a Telnet. Uchovává osobní

uživatelské profily síťového přístupu a automaticky je načítá ze serveru RADIUS či TACACS+ a posléze aplikuje.

Správa zásad cílových adres URL – sada funkcí, které se souhrnně označují jako filtrování adres URL.

Uživatelské firewally – v zásadě jde o přizpůsobené, uživatelsky specifické firewally ke stažení, které lze získat od poskytovatelů služeb. Přizpůsobené přístupové seznamy a další nastavení je také možné načíst z úložiště profilů serveru AAA.

Pořizování směrovačů a firewallů Cisco IOS – umožňuje automatické pořizování směrovačů, aktualizovaných verzí a zásad zabezpečení.

Detekce a prevence útoků DoS (denial of service) – funkce, která kontroluje hlavičky paketů a zahazuje všechny podezřelé pakety.

Dynamické mapování portu – typ adaptéru, který povoluje aplikace podporované firewallem na nestandardních portech.

Blokování apletů Java – chrání před zvláštními a nerozpoznanými aplety v jazyku Java.

Základní a rozšířené filtrování provozu

Cisco IOS Firewall umožňuje používat standardní, rozšířené a dokonce dynamické přístupové seznamy typu Lock-and-Key. Řízení přístupu lze nastavit v libovolném síťovém segmentu. Kromě toho je možné určit přesný typ provozu, který bude moci konkrétním segmentem procházet.

Podpora více rozhraní založená na zásadách – umožňuje řídit uživatelský přístup pomocí IP adresy a rozhraní v závislosti na zásadách zabezpečení.

Překlady adres NAT (Network Address Translation) – skrývá interní síť před vnějším okolím a tím zvyšuje zabezpečení. (O technologii NAT si povíme více v kapitole 11.)

Časové přístupové seznamy – určují zásady zabezpečení na základě přesného denního času a příslušného dne v týdnu.

Autentizace partnerských směrovačů – zaručuje, že směrovače budou získávat spolehlivé směrovací informace ze skutečných důvěryhodných zdrojů. (Předpokladem je směrovací protokol s podporou autentizace, jako např. RIPv2, EIGRP nebo OSPF.)

Když jste získali přehled o bezpečnostních hrozbách, příslušných funkcích produktu Cisco IOS Firewall a o tom, jak tento software využívat, zaměřme se podrobněji na oblast přístupových seznamů a ukažme si, jak lze pomocí přístupových seznamů omezit bezpečnostní hrozby. Tyto nástroje jsou skutečně účinné, takže jim věnujte dostatečnou pozornost.

Úvod do přístupových seznamů

Přístupový seznam (access list) je v praxi seznam podmínek, které charakterizují pakety. Mohou být mimořádně užitečné, potřebujete-li získat kontrolu nad síťovým provozem. Přístupový seznam bude v těchto situacích hlavním nástrojem pro rozhodování.

K nejčastějším a nesnáze pochopitelným aplikacím přístupových seznamů patří filtrování nežádoucích paketů při implementaci bezpečnostních zásad. Můžete je například nastavit tak, aby přijímaly velmi konkrétní rozhodnutí o regulaci schémat provozu, takže k webovým prostředkům v Internetu získají přístup pouze určití hostitelé, ale jiní budou mít přístup omezen. Správná kombinace přístupových seznamů dává správcům sítě schopnost vynutit téměř libovolnou zásadu zabezpečení, kterou si dokáží vymyslet.

Přístupové seznam lze uplatnit dokonce v situacích, které nutně nemusejí zahrnovat blokování paketů. Dovolují například řídit, které sítě budou či nebudou oznamovány pomocí dynamických směrovacích protokolů. Postup konfigurace přístupových seznamů je stejný. Rozdíl spočívá jednoduše v jejich aplikaci – místo na rozhraní v tomto případě na směrovací protokol. Při tomto použití se přístupový seznam označuje jako distribuční seznam a nezastavuje oznámení směrování, ale jen řídí jejich obsah. Přístupové seznamy také dovolují třídit pakety pro služby řazení do fronty nebo služby typu QoS a umožňují nastavit, které typy provozu mohou aktivovat nákladnou linku ISDN.

Vytváření přístupových seznamů se v praxi velmi podobá programování řady příkazů `if-then` – pokud je daná podmínka splněna, provede se příslušná akce. Jestliže konkrétní podmínka splněna není, nic se nestane a vyhodnotí se další příkaz. Příkazy přístupových seznamů jsou v zásadě filtry, podle kterých se porovnávají, třídí a zpracovávají pakety. Po vytvoření lze seznamy aplikovat na příchozí nebo odchozí provoz libovolného rozhraní. Při použití přístupového seznamu směrovač analyzuje každý paket, který prochází přes rozhraní v příslušném směru, a provede odpovídající akci.

Při porovnávání paketů podle přístupového seznamu platí několik důležitých pravidel:

- Paket se vždy porovnává s každým řádkem přístupového seznamu v pevném pořadí. To znamená, že se vždy začíná od prvního řádku přístupového seznamu, pak se přejde k řádku 2, poté řádku 3 atd.
- Porovnávání s řádky přístupového seznamu probíhá pouze tak dlouho, dokud není nalezena shoda. Jakmile paket odpovídá podmínce na řádku přístupového seznamu, je zpracován a k dalšímu porovnávání již nedochází.
- Na konci každého přístupového seznamu se nachází implicitní příkaz „deny“. Jestliže tedy paket nevyhovuje podmínce žádného řádku přístupového seznamu, je nakonec zahozen.

Každé z těchto pravidel pro filtrování paketů IP pomocí přístupových seznamů má určité závažné důsledky. Uvědomte si proto, že tvorba efektivních přístupových seznamů vyžaduje určitou praxi.

Přístupové seznamy se dělí na dva hlavní typy:

Standardní přístupové seznamy – tyto seznamy používají jako testovací podmínku pouze zdrojovou IP adresu v paketu IP. Všechna přijímaná rozhodnutí jsou založena na zdrojové IP adrese. To znamená, že standardní přístupové seznamy v zásadě povolují nebo zakazují celé sady protokolů. Nerozlišují mezi mnoha typy provozu IP, jako např. protokoly HTTP, Telnet, UDP atd.

Rozšířené přístupové seznam – rozšířené přístupové seznamy umožňují vyhodnocovat mnohá další pole v hlavičkách vrstvy 3 a 4 paketu IP. Mohou analyzovat zdrojovou a cílovou

IP adresu, pole protokolu v hlavičce síťové vrstvy a číslo portu v hlavičce transportní vrstvy. Rozšířené přístupové seznamy mohou díky tomu při řízení provozu uplatňovat mnohem jemnější pravidla.

Pojmenované přístupové seznamy – moment – před chvílí jsme uvedli, že existují dva typy přístupových seznamů, ale najednou uvádíme tři! Technicky jsou typy opravdu jen dva, protože *pojmenované přístupové seznamy* ve skutečnosti netvoří nový typ, ale jedná se buď o standardní, nebo o rozšířené přístupové seznamy. Budeme je však odlišovat proto, že se vytvářejí a odkazují odlišně než standardní a rozšířené přístupové seznamy, i když jsou funkčně stejné.

Poznámka

Podrobněji se na tyto typy přístupových seznamů podíváme dále v této kapitole.

Vytvořený přístupový seznam se nijak neprojeví, dokud jej neaplikujete. Tyto seznamy jsou skutečně uloženy ve směrovači, ale nejsou aktivní, dokud směrovači nesdělíte, co s nimi má provést. Chcete-li použít přístupový seznam jako filtr paketů, musíte jej aplikovat na rozhraní směrovače, kde chcete provoz filtrovat. Navíc je nutné určit směr provozu, pro který bude přístupový seznam účinný. To má svůj dobrý důvod – můžete požadovat odlišná pravidla pro odchozí provoz z podnikové sítě do Internetu, než pro příchozí provoz z Internetu do lokální sítě. Když tedy uvedete směr provozu, můžete – a často dokonce musíte – použít odlišné přístupové seznamy pro příchozí a odchozí provoz na jediném rozhraní:

Příchozí přístupové seznamy – když přístupový seznam aplikujete na příchozí pakety daného rozhraní, jsou tyto pakety pomocí přístupového seznamu zpracovány dříve, než jsou směrovány na odchozí rozhraní. Žádné odmítnuté pakety nejsou směrovány, protože jsou zahozeny ještě před tím, než proces směrování začne.

Odchozí přístupové seznamy – když přístupový seznam aplikujete na odchozí pakety daného rozhraní, jsou tyto pakety směrovány na odchozí rozhraní a poté pomocí přístupového seznamy zpracovány dříve, než jsou zařazeny do fronty.

Existuje několik obecných pravidel, která je vhodné dodržovat při vytváření a implementaci přístupových seznamů u směrovače:

- Můžete přiřadit pouze jeden přístupový seznam pro jedno rozhraní, protokol a směr. Z toho vyplývá, že při vytváření přístupových seznamů IP může existovat pouze jeden příchozí a jeden odchozí přístupový seznam týkající se konkrétního rozhraní.

Poznámka

Když se zamyslíte nad důsledky implicitního příkazu „deny" na konci každého přístupového seznamu, je pochopitelné, že pro stejné rozhraní, směr a protokol nelze aplikovat více přístupových seznamů. Všechny pakety, jež neodpovídají některé podmínce prvního přístupového seznamu, budou totiž zahozeny. Poté již nezůstanou žádné pakety, které by bylo možné porovnat s druhým přístupovým seznamem.

- Přístupové seznamy uspořádejte tak, aby byly konkrétnější testy na začátku.

- Každá nová položka, kterou přidáte do přístupového seznamu, je umístěna na jeho konec. Při úpravách přístupových seznamů je vhodné pracovat s textovým editorem.
- Z přístupového seznamu není možné odebrat jeden řádek. Pokud se o to pokusíte, smažete celý seznam. Než se seznam pokusíte měnit, je nejlepší zkopírovat jej do textového editoru. Jedinou výjimku představují pojmenované přístupové seznamy.

Poznámka

Z pojmenovaného přístupového seznamu lze odstranit jediný řádek. Zakrátko si to ukážeme.

- Pokud přístupové seznamy nezakončíte příkazem `permit any`, budou zahozeny všechny pakety, které nesplní žádný z testů seznamu. Každý seznam by měl mít alespoň jeden příkaz `permit`, protože jinak zakáže veškerý provoz.
- Vytvořte přístupové seznamy a poté je aplikujte na rozhraní. Přístupový seznam použitý na rozhraní bez aktuálního přístupového seznamu nebude filtrovat provoz.
- Přístupové seznamy jsou navrženy tak, aby filtrovaly provoz procházející přes směrovač. Nefiltrují provoz, který je generován směrovačem.
- Standardní přístupové seznamy IP umístěte co nejblíže jejich cílovému umístění. Z tohoto důvodu zpravidla není vhodné v sítích používat standardní přístupové seznamy. Standardní přístupový seznam není možné umístit blízko zdrojového hostitele nebo sítě, protože dokáží filtrovat pouze podle zdrojových adres a nebylo by možné žádná data předat dále.
- Rozšířené přístupové seznamy IP umístěte co nejblíže zdrojovému umístění. Rozšířené přístupové seznamy umožňují filtrovat podle velmi konkrétních adres a protokolů. Není tedy žádoucí, aby data procházela celou sítí a nakonec byla zahozena. Umístíte-li tento seznam co nejblíže zdrojové adrese, můžete provoz filtrovat dříve, než začne konzumovat cennou šířku pásma sítě.

Než se pustíme do konfigurace základních a pokročilých rozšířených seznamů, rozeberme si, jak mohou přístupové seznamy zmírňovat bezpečnostní hrozby uvedené v předchozí části této kapitoly.

Potlačení bezpečnostních hrozeb s přístupovými seznamy

Následuje seznam mnoha bezpečnostních hrozeb, před kterými mohou přístupové seznamy chránit:

- Falšování IP adres, příchozí
- Falšování IP adres, odchozí
- Útoky DoS (denial of service) typu TCP SYN, blokování externích útoků
- Útoky DoS (denial of service) typu TCP SYN, použití zachycení TCP
- Útoky DoS smurf

- Filtrování zpráv ICMP, příchozí
- Filtrování zpráv ICMP, odchozí
- Filtrování příkazu traceroute

Obecně je rozumné nepouštět do privátní sítě žádné pakety IP, které obsahují zdrojovou adresu jakéhokoli interního hostitele či sítě – rozhodně se tomu vyhněte!

Uveďme si seznam pravidel, která je kvůli zmírnění bezpečnostních rizik dobré dodržovat při konfiguraci přístupových seznamů pro provoz směřující z Internetu do produkční sítě:

- Odmítněte všechny adresy ze svých interních sítí.
- Odmítněte všechny adresy místních hostitelů (127.0.0.0/8).
- Odmítněte všechny rezervované privátní adresy.
- Odmítněte všechny adresy v rozsahu adres vícesměrového vysílání IP (224.0.0.0/4).

Do své datové sítě byste neměli pouštět data pocházející ze žádné z výše uvedených adres. Nyní se tedy můžeme pustit do konfigurace několika základních a pokročilých přístupových seznamů.

Standardní přístupové seznamy

Standardní přístupové seznamy IP filtrují síťový provoz na základě zdrojové IP adresy v paketu. *Standardní přístupové seznamy IP* lze vytvářet s čísly access-list 1–99 nebo 1 300–1 999 (rozšířený rozsah). Typy přístupových seznamů se obvykle odlišují pomocí čísel. V závislosti na čísle použitém při vytvoření přístupového seznamu směrovač ví, který typ syntaxe má při zadávání seznamu očekávat. Pomocí čísel z rozsahu 1–99 nebo 1 300–1 999 informujete směrovač, že chcete vytvořit standardní přístupový seznam IP. Směrovač tedy bude na testovacích řádcích očekávat syntaxi, která definuje pouze zdrojovou IP adresu.

Následuje příklad mnoha číselných rozsahů příkazu access-list, pomocí nichž lze filtrovat síťový provoz (protokoly, pro které je možné nastavit přístupové seznamy, závisejí na verzi systému IOS):

```
Corp(config)#access-list ?
  <1-99>             IP standard access list
  <100-199>          IP extended access list
  <1100-1199>        Extended 48-bit MAC address access list
  <1300-1999>        IP standard access list (expanded range)
  <200-299>          Protocol type-code access list
  <2000-2699>        IP extended access list (expanded range)
  <700-799>          48-bit MAC address access list
  compiled           Enable IP access-list compilation
  dynamic-extended   Extend the dynamic ACL absolute timer
  rate-limit         Simple rate-limit specific access list
```

Podívejme se na syntaxi, která se používá při vytváření standardních přístupových seznamů:

```
Corp(config)#access-list 10 ?
deny                Specify packets to reject
permit              Specify packets to forward
remark              Access list entry comment
```

Jak jsme již uvedli, z čísel access-list 1–99 nebo 1 300–1 999 směrovač zjistí, že chcete vytvořit standardní přístupový seznam IP. Po výběru čísla access-list se musíte rozhodnout, zda budete vytvářet příkaz `permit` nebo `deny`. V tomto příkladu vytvoříme příkaz `deny`:

```
Corp(config)#access-list 10 deny ?
Hostname or A.B.C.D       Address to match
any                       Any source host
host                      A single host address
```

Další krok vyžaduje podrobnější vysvětlení. K dispozici jsou tři možnosti. Pomocí parametru `any` lze povolit nebo zakázat libovolného hostitele nebo síť. IP adresa umožňuje uvést jediného hostitele nebo jejich rozsah, případně je možné příkazem `host` specifikovat konkrétního hostitele. Příkaz `any` je snadno pochopitelný – příkazu vyhovuje libovolná zdrojová adresa, takže se s tímto řádkem bude shodovat každý porovnávaný paket. Příkaz `host` je poměrně prostý. Uveďme si příklad jeho použití:

```
Corp(config)#access-list 10 deny host ?
  Hostname or A.B.C.D Host address
Corp(config)#access-list 10 deny host 172.16.30.2
```

Na základě tohoto příkazu seznam odmítne všechny pakety z hostitele 172.16.30.2. Výchozí parametr je `host`. Jinými slovy pokus zadáte příkaz `access-list 10 deny 172.16.30.2`, směrovač předpokládá, že máte na mysli hostitele 172.16.30.2.

Konkrétního hostitele nebo jejich rozsah lze však definovat i jinak – pomocí maskování zástupných znaků. Chcete-li v praxi specifikovat jakýkoli rozsah hostitelů, musíte v přístupovém seznamu použít maskování zástupných znaků.

Co to je maskování zástupných znaků? V následujících sekcích si to vysvětlíme na příkladu standardního přístupového seznamu a ukážeme si také, jak řídit přístup k virtuálnímu terminálu.

Zástupné masky

Zástupné znaky v přístupových seznamech určují jednotlivého hostitele, síť nebo konkrétní rozsah sítě či sítí. Chcete-li rozumět pojmu *zástupný znak* (wildcard), musíte chápat význam *velikosti bloku*, která udává rozsah adres. Dostupné jsou například tyto velikosti bloku: 64, 32, 16, 8 a 4.

Jestliže potřebujete určit rozsah adres, zvolíte následující větší velikost bloku, která odpovídá vašim požadavkům. Pokud chcete definovat 34 sítí, potřebujete velikost bloku 64. V případě 18 hostitelů vyhovuje velikost bloku 32. Jestliže specifikujete jen 2 sítě, postačí velikost bloku 4.

Zástupné znaky u hostitelské nebo síťové adresy informují směrovač o rozsahu dostupných adres pro filtrování. Chcete-li určit hostitele, bude adresa vypadat takto:

```
172.16.30.5 0.0.0.0
```

Čtyři nuly představují jednotlivé oktety adresy. Kdykoli je uvedena nula, znamená to, že oktet v adrese se musí přesně shodovat. Pokud chcete nastavit, že oktet může mít libovolnou hodnotu, zadejte místo nuly číslo 255. Následující příklad ukazuje, jak lze pomocí zástupných znaků definovat podsíť /24:

```
172.16.30.0 0.0.0.255
```

Tento zápis směrovači sděluje, aby vyhledal přesnou shodu v prvních třech oktetech, ale poslední oktet může mít libovolnou hodnotu.

Tato část byla snadná. Jak ale postupovat, chcete-li definovat pouze malý rozsah podsítí? Zde se uplatní velikosti bloku. Musíte určit rozsah hodnot ve velikosti bloku. Jinými slovy se nemůžete rozhodnout, že nastavíte 20 sítí. Můžete uvést jen počet, který se přesně shoduje s velikostí bloku. Rozsah se může například rovnat 16 nebo 32, ale nikoli 20.

Řekněme, že chcete blokovat přístup do části sítě, která leží v rozsahu od 172.16.8.0 do 172.16.15.0. To odpovídá velikosti bloku 8. Číslo sítě bude 172.16.8.0 a zástupný znak bude mít tvar 0.0.7.255. Co to je? Podle čísel 7.255 směrovač zjistí velikost bloku. Hodnoty sítě a zástupného znaku informují směrovač, aby začal na adrese 172.16.8.0 a postupoval po velikosti bloku s osmi adresami k síti 172.16.15.0.

Opravdu je to snazší, než se zdá! Mohli bychom si předvést příslušnou binární matematiku, ale není to nutné. V praxi stačí, když si budete pamatovat, že zástupný znak je vždy o jednotku menší než velikost bloku. V našem příkladu tedy bude mít zástupný znak hodnotu 7, protože velikost bloku se rovná 8. Pokud bychom používali bloky velikosti 16, zástupný znak by byl 15. Nic na tom není, že?

Pro jistotu si však projdeme několik příkladů, abyste si vše dobře osvojili. Následující příklad směrovači sděluje, aby vyhledal přesnou shodu v prvních třech oktetech, ale na čtvrtém oktetu nezáleží:

```
Corp(config)#access-list 10 deny 172.16.10.0 0.0.0.255
```

V dalším příkladu směrovač páruje podle prvních dvou oktetů a poslední dva oktety mohou být libovolné:

```
Corp(config)#access-list 10 deny 172.16.0.0
  0.0.255.255
```

Pokuste se přijít na význam následujícího příkazu:

```
Corp(config)#access-list 10 deny 172.16.16.0 0.0.3.255
```

Tato konfigurace zajistí, že směrovač začne u sítě 172.16.16.0 a bude používat velikost bloku 4. Rozsah poté bude 172.16.16.0 až 172.16.19.0.

Následující příklad představuje přístupový seznam, který začíná na adrese 172.16.16.0 a pokračuje po blocích velikosti 8 do adresy 172.16.23.0:

```
Corp(config)#access-list 10 deny 172.16.16.0 0.0.7.255
```

Následující ukázka začíná sítí 172.16.32.0 a po blocích velikosti 16 postupuje k adrese 172.16.47.0:

```
Corp(config)#access-list 10 deny 172.16.32.0 0.0.15.255
```

Další příklad začíná sítí 172.16.64.0 a poté po blocích velikosti 64 končí adresou 172.16.127.0:

```
Corp(config)#access-list 10 deny 172.16.64.0 0.0.63.255
```

Poslední příklad začíná sítí 192.168.160.0 a následně adresu inkrementuje o bloky velikosti 32 až do adresy 192.168.191.255:

```
Corp(config)#access-list 10 deny 192.168.160.0 0.0.31.255
```

Při práci s velikostmi bloků a zástupnými znaky je potřeba mít na paměti ještě dvě věci:

- Každá adresa musí začínat nulou nebo násobkem velikosti bloku. Nelze například zvolit velikost bloku 8 a poté začít hodnotou 12. Je nutné uvést hodnoty 0–7, 8–15, 16–23 atd. V případě bloku velikosti 32 se jedná o rozsahy 0–31, 32–63, 64–95 atd.
- Příkaz `any` je ekvivalentní zápisu zástupného znaku 0.0.0.0 255.255.255.255.

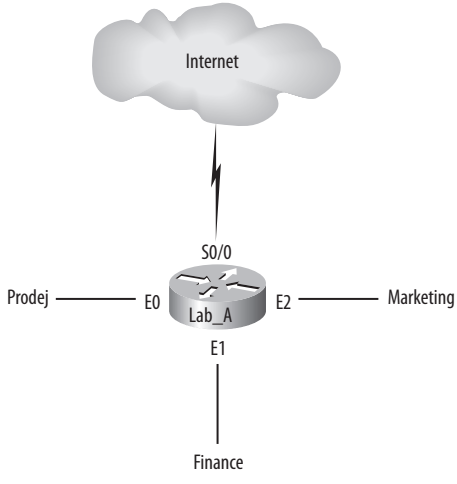
Poznámka

Chcete-li vytvářet přístupové seznamy IP, neobejdete se bez zvládnutí maskování zástupných znaků. Při vytváření standardních a rozšířených přístupových seznamů IP se postupuje shodně.

Příklad standardního přístupového seznamu

V této sekci se dozvíte, jak lze pomocí standardního přístupového seznamu zabránit určitým uživatelům v přístupu do sítě LAN oddělení Finance.

Směrovač na obrázku 10.2 má tři připojení LAN a jedno připojení WAN do Internetu. Uživatelé v síti LAN Prodej by neměli mít přístup do lokální sítě Finance, ale měli by mít přístup k Internetu a oddělení Marketing. Lokální síť Marketing potřebuje přístup k síti LAN Finance kvůli aplikačním službám.



Obrázek 10.2: Příklad přístupového seznamu IP se třemi připojeními LAN a jedním připojením WAN

U směrovače na obrázku je nakonfigurován následující standardní přístupový seznam IP:

```
Lab_A#config t
Lab_A(config)#access-list 10 deny 172.16.40.0 0.0.0.255
Lab_A(config)#access-list 10 permit any
```

Je velmi důležité vědět, že příkaz `any` znamená totéž jako následující zápis s maskováním zástupných znaků:

```
Lab_A(config)#access-list 10 permit 0.0.0.0
255.255.255.255
```

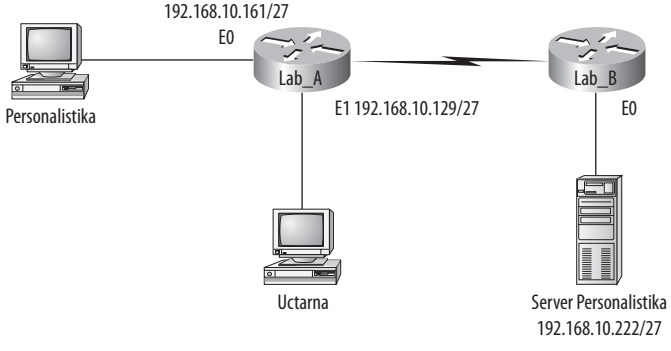
Maska zástupných znaků neuvádí žádné oktety pro vyhodnocení, takže testovací podmínce vyhovují všechny adresy. Funkčně se tedy jedná o stejný příkaz jako u klíčového slova `any`.

V této fázi je přístupový seznam nakonfigurován tak, aby odmítl přístup do lokální sítě Finance ze zdrojových adres v lokální síti Prodej a povolil přístup všem ostatním. Pamatujte však, že se neprovede žádná akce, dokud není přístupový seznam aplikován na rozhraní v konkrétním směru. Kam je však potřeba tento přístupový seznam umístit? Pokud jej umístíte jako příchozí přístupový seznam rozhraní E0, můžete rozhraní Ethernet zrovna vypnout, protože všem zařízením v lokální síti Prodej odepřete přístup do všech sítí připojených ke směrovači. Tento přístupový seznam je nejvhodnější nastavit na rozhraní E1 jako odchozí seznam:

```
Lab_A(config)#int e1
Lab_A(config-if)#ip access-group 10 out
```

Tím zcela zastavíte odchozí provoz z adresy 172.16.40.0 přes rozhraní Ethernet 1. Nastavení nijak neovlivní přístup hostitelů z lokální sítě Prodej do sítě Marketing a do Internetu, protože provoz do těchto cílových umístění neprochází přes rozhraní E1. Každý paket, který je určen k odeslání z rozhraní E1, musí nejdříve projít kontrolou podle přístupového seznamu. Pokud byste na rozhraní E0 umístili příchozí seznam, musely by všechny pakety vstupující na rozhraní E0 nejdříve absolvovat kontrolu podle přístupového seznamu, aby mohly být následně směrovány na výstupní rozhraní.

Podívejme se na další ukázku standardního přístupového seznamu. Obrázek 10.3 znázorňuje datovou síť se dvěma směrovači, třemi sítěmi LAN a jedním sériovým připojením WAN.



Obrázek 10.3: Příklad standardního přístupového seznamu č. 2

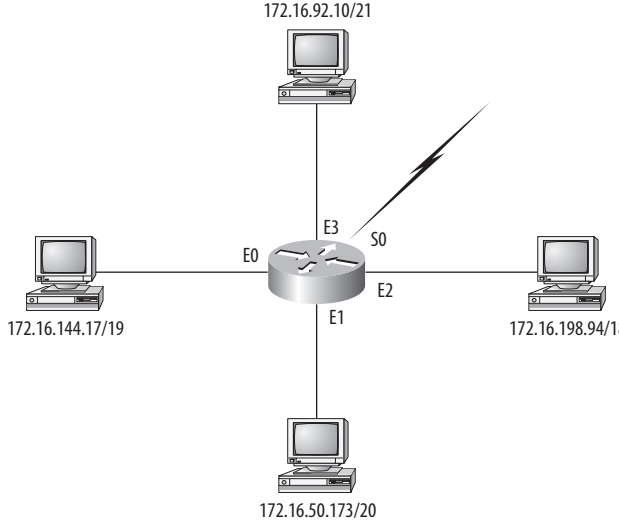
Chcete uživatelům sítě Uctarna zabránit v přístupu k serveru Personalistika připojenému ke směrovači Lab_B, ale povolit přístup k dané síti LAN všem ostatním uživatelům. Jaký standardní přístupový seznam vytvoříte a kam jej umístíte?

V praxi by bylo lepší použít rozšířený přístupový seznam a umístit jej blíže ke zdroji, ale zadání požaduje, abyste použili standardní přístupový seznam. Standardní přístupové seznamy se zpravidla umisťují blíže k cíli – v tomto případě na odchozí rozhraní Ethernet 0 směrovače Lab_B. Přístupový seznam, který je potřeba nastavit u směrovače Lab_B, vypadá takto:

```
Lab_B#config t
Lab_B(config)#access-list 10 deny 192.168.10.128 0.0.0.31
Lab_B(config)#access-list 10 permit any
Lab_B(config)#interface Ethernet 0
Lab_B(config-if)#ip access-group 10 out
```

Než přejdeme k omezení přístupu ke směrovači protokolem Telnet, podívejme se ještě na jeden příklad standardního přístupového seznamu, který je však poněkud náročnější na pochopení. Na obrázku 10.4 je znázorněn směrovač se čtyřmi připojeními LAN a jedním připojením WAN do Internetu.

Potřebujete napsat přístupový seznam, který zastaví přístup do Internetu z každé ze čtyřech sítí LAN ve schématu. Každá z lokálních sítí zobrazuje IP adresu jediného hostitele a z této hodnoty musíte určit podsíť a pomocí zástupných znaků nakonfigurovat přístupový seznam.



Obrázek 10.4: Příklad standardního přístupového seznamu č. 3

Následuje příklad možné správné odpovědi (počínaje sítí na rozhraní E0 a konče sítí na rozhraní E3):

```
Router(config)#access-list 1 deny 172.16.128.0 0.0.31.255
Router(config)#access-list 1 deny 172.16.48.0 0.0.15.255
Router(config)#access-list 1 deny 172.16.192.0 0.0.63.255
Router(config)#access-list 1 deny 172.16.88.0 0.0.7.255
Router(config)#access-list 1 permit any
Router(config)#interface serial 0
Router(config-if)#ip access-group 1 out
```

Jaký význam by mělo vytvoření tohoto seznamu? Pokud byste v praxi aplikovali tento přístupový seznam na směrovač, znemožnili byste tím přístup k Internetu. K čemu byste tedy vůbec internetové připojení potřebovali? Toto cvičení slouží jen k tomu, abyste si mohli procvičit použití velikostí bloku s přístupovými seznamy, což je zásadně důležité při studiu okruhů zkoušky CCNA.

Kontrola přístupu k lince VTY (Telnet)

Nejspíš těžko zabráníte uživatelům, aby se k velkému směrovači přihlašovali protokolem Telnet, protože každé aktivní rozhraní směrovače představuje snadný cíl pro přístup VTY. Můžete se pokusit o vytvoření rozšířeného přístupového seznamu IP, který omezí přístup typu Telnet na každou IP adresu směrovače. Pokud to však uděláte, musíte tento seznam aplikovat jako příchozí na každém rozhraní. Takové řešení by se rozhodně nehodilo pro velký směrovač s desítkami či dokonce stovkami rozhraní. Existuje však mnohem lepší varianta: Pomocí standardního přístupového seznamu IP lze řídit přístup k vlastním linkám VTY.

Proč to funguje? Když totiž aplikujete přístupový seznam na linky VTY, nemusíte uvádět protokol Telnet, protože přístup k lince VTY implikuje terminálový přístup. Není nutné specifikovat ani cílovou adresu. V praxi totiž vůbec nezáleží na tom, kterou adresu rozhraní uživatel zvolí jako cíl relace Telnet. Stačí pouze kontrolovat, odkud uživatel přichází – tedy zdrojovou IP adresu.

Chcete-li použít tuto funkci, postupujte následovně:

1. Vytvořte standardní přístupový seznam IP, který povolí jen hostitele, jimž chcete umožnit připojení ke směrovači protokolem Telnet.
2. Aplikujte přístupový seznam na linku VTY příkazem `access-class`.

Uveďme si příklad, jak povolit přihlášení ke směrovači protokolem Telnet pouze hostiteli 172.16.10.3:

```
Lab_A(config)#access-list 50 permit 172.16.10.3
Lab_A(config)#line vty 0 4
Lab_A(config-line)#access-class 50 in
```

Z praxe

Je vhodné u směrovače zabezpečit linky Telnet?

Sledujete svou síť a všimnete si, že se někdo přihlásil k centrálnímu směrovači protokolem Telnet pomocí příkazu `show users`. Zadáte příkaz `disconnect`, abyste uživatele odpojili od směrovače, ale o několik minut později je uživatel přihlášen znovu. Uvažujete o tom, že byste na rozhraní směrovače umístili přístupové seznamy, ale nechcete příliš zvyšovat latenci jednotlivých rozhraní, protože směrovač je již poměrně vytížen přenosem paketů. Přemýšlíte nad tím, že byste umístili přístupový seznam na vlastní linky VTY. Zatím jste to však nedělali a proto si nejste jisti, zda tento postup představuje bezpečnou alternativu k nastavení přístupových seznamů pro každé rozhraní. Je umístění přístupového seznamu na linky VTY v této síti rozumné?

Rozhodně – a nejlepší postup představuje příkaz `access-class`, kterým se zabýváme v této sekci. Proč? Nepoužívá totiž přístupový seznam, který by analyzoval každý paket procházející přes rozhraní v jednom či druhém směru. Tento postup může zvýšit režii směrování paketů.

Když však umístíte příkaz `access-class` na linky VTY, zajistíte tím, že se budou analyzovat a porovnávat pouze pakety, které jsou určeny pro připojení ke směrovači protokolem Telnet. Elegantně tím dosáhnete bezpečného nastavení směrovače, které se snadno konfiguruje.

Vzhledem k implicitnímu příkazu `deny any` na konci seznamu znemožní přístupový seznam připojení ke směrovači protokolem Telnet každému hostiteli, s výjimkou hostitele 172.16.10.3. Nezáleží při tom na tom, která z jednotlivých IP adres směrovače se používá jako cílová.

Tip

Společnost Cisco doporučuje, abyste se na linkách VTY směrovače připojovali místo protokolu Telnet raději pomocí SSH (Secure Shell). Další informace o protokolu SSH a jeho konfiguraci u směrovačů a přepínačů naleznete v kapitole 4.

Rozšířené přístupové seznamy

V příkladu se standardním přístupovým seznamem IP výše si všimněte, jak jsme museli zablokovat veškerý přístup z lokální sítě Prodej do sítě finančního oddělení. Jak ale postupovat v případě, že by zaměstnanci oddělení Prodej potřebovali přístup k některému serveru v lokální síti Finance, ale z bezpečnostních důvodů by nesměli přistupovat k ostatním síťovým službám? U standardních přístupových seznamů IP nelze uživatelům povolit přístup k jedné síťové službě, ale odepřít přístup k jiné. Jinak řečeno: potřebujete-li se rozhodovat na základě zdrojové i cílové adresy, standardní přístupový seznam to neumožní, protože přijímá rozhodnutí pouze v závislosti na zdrojové adrese.

Problém je ale možné vyřešit *rozšířeným přístupovým seznamem*. Rozšířené přístupové seznamy totiž dovolují určit zdrojovou a cílovou adresu a rovněž protokol a číslo portu, které identifikují protokol či aplikaci vyšší vrstvy. Pomocí rozšířených přístupových seznamů můžete účinně povolit uživatelům přístup do fyzické sítě LAN a zakázat jim přístup ke konkrétním hostitelům – nebo dokonce určitým službám těchto hostitelů.

Uveďme si příklad rozšířeného přístupového seznamu IP:

```
Corp(config)#access-list ?
  <1-99>              IP standard access list
  <100-199>           IP extended access list
  <1100-1199>         Extended 48-bit MAC address access list
  <1300-1999>         IP standard access list (expanded range)
  <200-299>           Protocol type-code access list
  <2000-2699>         IP extended access list (expanded range)
  <700-799>           48-bit MAC address access list
  compiled            Enable IP access-list compilation
  dynamic-extended    Extend the dynamic ACL absolute timer
  rate-limit          Simple rate-limit specific access list
```

První příkaz zobrazuje dostupná čísla access-list. Zvolíme rozšířený rozsah od 100 do 199. Všimněte si, že pro rozšířené přístupové seznamy IP je k dispozici i rozsah 2 000–2 699.

V této fázi se musíte rozhodnout, jaký typ položky seznamu vytváříte. V tomto příkladu vybereme položku seznamu `deny`.

```
Corp(config)#access-list 110 ?
  deny        Specify packets to reject
  dynamic     Specify a DYNAMIC list of PERMITs or DENYs
```

```
  permit      Specify packets to forward
  remark      Access list entry comment
```

Jakmile zvolíte typ access-list, musíte vybrat položku pole protokolu.

```
Corp(config)#access-list 110 deny ?
  <0-255>     An IP protocol number
  ahp         Authentication Header Protocol
  eigrp       Cisco's EIGRP routing protocol
  esp         Encapsulation Security Payload
  gre         Cisco's GRE tunneling
  icmp        Internet Control Message Protocol
  igmp        Internet Gateway Message Protocol
  ip          Any Internet Protocol
  ipinip      IP in IP tunneling
  nos         KA9Q NOS compatible IP over IP tunneling
  ospf        OSPF routing protocol
  pcp         Payload Compression Protocol
  pim         Protocol Independent Multicast
  tcp         Transmission Control Protocol
  udp         User Datagram Protocol
```

Poznámka

Chcete-li filtrovat podle protokolu aplikační vrstvy, musíte za příkazem `permit` **nebo** `deny` **zvolit příslušný transportní protokol vrstvy 4. Při filtrování provozu Telnet či FTP například zvolíte TCP, protože protokoly Telnet i FTP používají na transportní vrstvě protokol TCP. Kdybyste vybrali protokol IP, nemohli byste později určit konkrétní aplikační protokol.**

Zde si výběrem protokolu TCP zvolíte filtrování protokolu aplikační vrstvy, který používá protokol TCP. Konkrétní port protokolu TCP určíte později. Dále se zobrazí výzva k zadání zdrojové IP adresy hostitele nebo sítě (chcete-li povolit libovolnou zdrojovou adresu, uveďte příkaz `any`):

```
Corp(config)#access-list 110 deny tcp ?
  A.B.C.D     Source address
  any         Any source host
  host        A single source host
```

Po výběru zdrojové adresy je potřeba zvolit cílovou adresu:

```
Corp(config)#access-list 110 deny tcp any ?
  A.B.C.D     Destination address
  any         Any destination host
  eq          Match only packets on a given port number
  gt          Match only packets with a greater port number
  host        A single destination host
  lt          Match only packets with a lower port number
  neq         Match only packets not on a given port number
  range       Match only packets in the range of port numbers
```

Následující příklad zajistí odmítnutí každé zdrojové IP adresy, která má cílovou IP adresu 172.16.30.2.

```
Corp(config)#access-list 110 deny tcp any host 172.16.30.2 ?
  ack              Match on the ACK bit
  dscp             Match packets with given dscp value
  eq               Match only packets on a given port number
  established      Match established connections
  fin              Match on the FIN bit
  fragments        Check non-initial fragments
  gt               Match only packets with a greater port number
  log              Log matches against this entry
  log-input        Log matches against this entry, including input interface
  lt               Match only packets with a lower port number
  neq              Match only packets not on a given port number
  precedence       Match packets with given precedence value
  psh              Match on the PSH bit
  range            Match only packets in the range of port numbers
  rst              Match on the RST bit
  syn              Match on the SYN bit
  time-range       Specify a time-range
  tos              Match packets with given TOS value
  urg              Match on the URG bit
  <cr>
```

Nyní můžete stisknout klávesu Enter a přístupový seznam dále neměnit. V tomto případě však budete odmítat veškerý provoz protokolu TCP směřující na hostitele 172.16.30.2, bez ohledu na cílový port. Můžete být dokonce ještě konkrétnější: Jakmile máte připraveny hostitelské adresy, stačí zadat typ blokované služby.

Následující obrazovka nápovědy shrnuje dostupné možnosti. Je možné zvolit číslo portu nebo použít název aplikace či protokolu:

```
Corp(config)#access-list 110 deny tcp any host 172.16.30.2 eq ?
  <0-65535>        Port number
  bgp              Border Gateway Protocol (179)
  chargen          Character generator (19)
  cmd              Remote commands (rcmd, 514)
  daytime          Daytime (13)
  discard          Discard (9)
  domain           Domain Name Service (53)
  drip             Dynamic Routing Information Protocol (3949)
  echo             Echo (7)
  exec             Exec (rsh, 512)
  finger           Finger (79)
  ftp              File Transfer Protocol (21)
  ftp-data         FTP data connections (20)
  gopher           Gopher (70)
  hostname         NIC hostname server (101)
  ident            Ident Protocol (113)
  irc              Internet Relay Chat (194)
  klogin           Kerberos login (543)
```

```
kshell          Kerberos shell (544)
login           Login (rlogin, 513)
lpd             Printer service (515)
nntp            Network News Transport Protocol (119)
pim-auto-rp     PIM Auto-RP (496)
pop2            Post Office Protocol v2 (109)
pop3            Post Office Protocol v3 (110)
smtp            Simple Mail Transport Protocol (25)
sunrpc          Sun Remote Procedure Call (111)
syslog          Syslog (514)
tacacs          TAC Access Control System (49)
talk            Talk (517)
telnet          Telnet (23)
time            Time (37)
uucp            Unix-to-Unix Copy Program (540)
whois           Nicname (43)
www             World Wide Web (HTTP, 80)
```

Vyzkoušejme v této fázi zablokovat protokol Telnet (port 23) pouze hostiteli 172.16.30.2. Uživatelé se i nadále mohou přihlásit protokolem FTP, který zůstává povolen. Příkaz `log` umožňuje protokolovat zprávy při každé aplikaci přístupového seznamu. Může se jednat o mimořádně praktický způsob, jak sledovat neoprávněné pokusy o přístup. Postupujte přitom takto:

```
Corp(config)#access-list 110 deny tcp any host 172.16.30.2 eq 23 log
```

Musíte pamatovat, že další řádek představuje ve výchozím nastavení implicitní příkaz `deny any`. Jestliže tento přístupový seznam aplikujete na rozhraní, můžete rozhraní stejně dobře úplně vypnout, protože na konci každého přístupového seznamu se nachází implicitní příkaz `deny all`. Přístupový seznam je nutné doplnit tímto příkazem:

```
Corp(config)#access-list 110 permit ip any any
```

Nezapomínejte, že zápis `0.0.0.0 255.255.255.255` představuje stejný příkaz jako `any`, takže by příkaz mohl vypadat následovně:

```
Corp(config)#access-list 110 permit ip 0.0.0.0 255.255.255.255
0.0.0.0 255.255.255.255
```

Jakmile vytvoříte přístupový seznam, musíte jej aplikovat na rozhraní (obdobně jako standardní seznam IP):

```
Corp(config-if)#ip access-group 110 in
```

Nebo:

```
Corp(config-if)#ip access-group 110 out
```

V následující sekci se podíváme na příklad použití rozšířeného přístupového seznamu.

Příklad rozšířeného přístupového seznamu 1

Budeme vycházet z obrázku 10.2 z příkladu na standardní přístupový seznam IP. Ve stejné síti odepřeme přístup k hostiteli s adresou 172.16.30.5 v lokální síti oddělení Finance pro služby