Cisco IOS Firewall

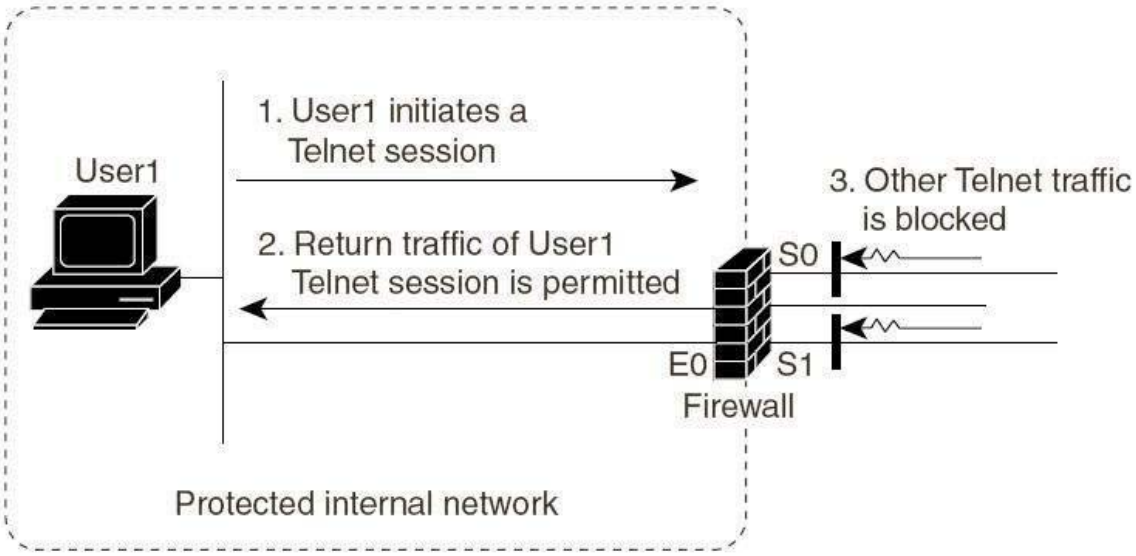
Množina funkcí Cisco IOS Firewallu

Cisco IOS Firewall poskytuje integrované funkce firewallu a tím zvyšuje flexibilitu a bezpečnost Cisco routeru.
Stručný přehled jeho nejdůležitějších vlastností:

- **Kontextově závislé řízení přístupu CBAC –** Interním uživatelům nabízí bezpečné řízení přístupu podle jednotlivých aplikací, podléhá mu veškerý provoz sítě.
- **Detekce vniknutí –** Okamžité monitorování, zadržení a reakce na zneužití sítě. Detekce je postavena na množině signatur reprezentující nejběžnější typy útoků.
- **Detekce a prevence útoků odepřením služeb –** Brání a ochraňuje prostředky routeru a strojů v sítí proti běžným útokům; kontroluje hlavičky paketů a podezřelé pakety zahazuje.
- **Blokování java appletů –** Chrání síť proti zlomyslným java appletům.
- **Okamžitá varovná hlášení –** V reálném čase zaznamenává varování o útocích.
- **Záznam auditu –** Podrobné sledování provozu; pro podrobné sestavy zaznamenává časové razítko, zdrojový hostitelský systém, cílový hostitelský systém, porty, dobu trvání a celkový počet přenesených bajtů.
- **Záznam událostí –** Pomocí záznamu událostí může síťový administrátor sledovat v reálném čase potencionální prolomení bezpečnosti a jiné nestandardní aktivity.
- **Autentizace partnerských routerů –** V routeru zajišťuje příjem paketů jen od důvěryhodných zdrojů.
- **…**

Činnost kontextově závislého řízení přístupu CBAC

Jestliže síťový provoz vystupuje z interní sítě skrze firewall,vytváří pro něj mechanismus CBAC v přístupových seznamech příslušných rozhraní firewallu dočasný průchod. Tento průchod umožňuje zpětný tok provozu, jež by byl normálně blokován, a vytváří další datové kanály pro zpětný vstup do interní sítě přes firewall. CBAC navíc povoluje průchod do interní sítě pouze tehdy, pokud je součástí stejné komunikační relace jako původní provoz, který činnost CBAC při výstupu z firewallu vyvolal.
Na *obrázku č.1* je příklad relace procházející přes CBAC, v tomto případě relace Telnet, obecně to však platí pro jakoukoliv komunikační relaci.



Obrázek č.1 – Činnost kontextově závislého řízení přístupu CBAC
Cisco IOS Security Configuration Guide, str 267.

Popis:

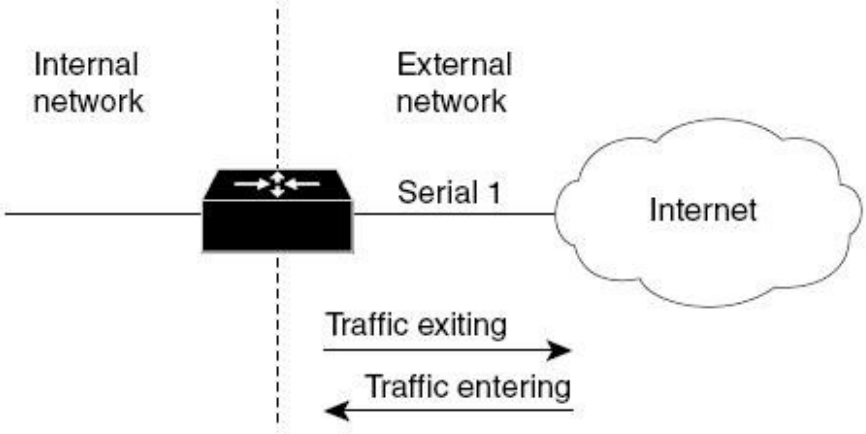
- Uživatel zahájí relaci Telnet (obecně CBAC může monitorovat jednokanálové i generické komunikace v protokolu TCP či UDP)
- CBAC povolí průchod zpětného provozu z relace Telnet uživatele
- Ostatní provoz Telnet externího původu CBAC zablokuje

Pro konfiguraci CBAC se musí aplikovat následujících několik kroků:

Výběr rozhraní pro CBAC – Nejprve se musí zvolit příslušné rozhraní pro CBAC, tj. jestli konfigurovat CBAC nad interním nebo externím rozhraním firewallu. Interní rozhraní znamená tu stranu, ze které budou vycházet relace, jejichž provoz nebude blokován, zatímco u externího rozhraní ano.

Konfigurace přístupových seznamů nad rozhraním
Firewall je nejběžněji užíván v jedné ze dvou základních topologií. Určení, které z těchto topologií je nejpodobnější konkrétní topologii, může napomoci při rozhodování, zda konfigurovat CBAC nad externím čí interním rozhraním.

První topologie, která je na *obrázku č.2*, je topologie, kde je CBAC konfigurováno nad **externím** rozhraním.



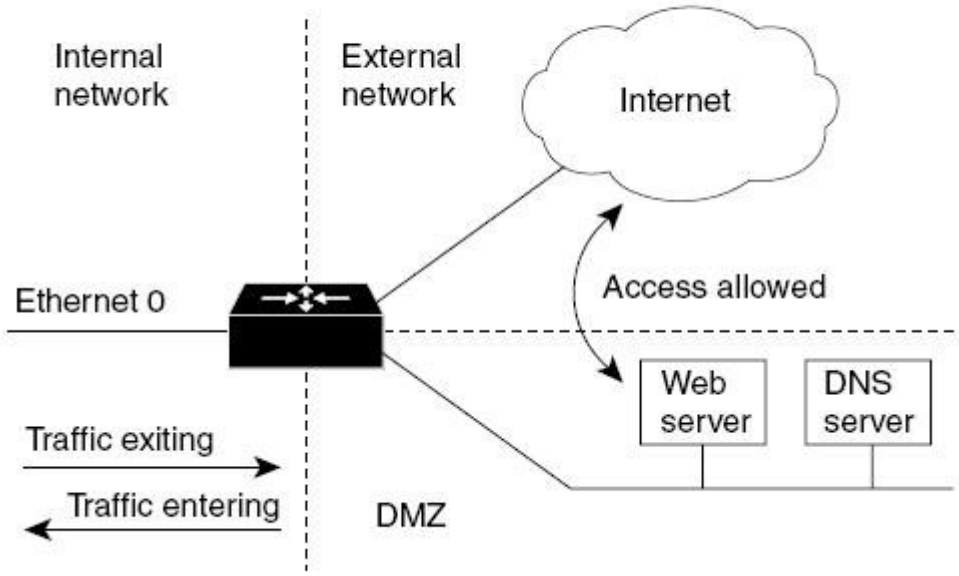
Obrázek č.2 – Konfigurace CBAC nad externím rozhraní
Cisco IOS Security Configuration Guide, str 275.

Popis:

- Provoz vstupující do firewallu z externí sítě bude blokován mimo ten, který je součástí komunikační relace inicializované v interní síti.

Pokud je nad externím rozhraním definován odchozí (z rozhraní do internetu) přístupový seznam, může tento seznam povolovat síťový provoz, který bude podléhat kontrole CBAC, pokud by provoz povolen nebyl, nepodléhal by inspekci CBAC a pakety by byly jednoduše zahozeny.
Příchozím přístupovým seznamem nad externím rozhraním musí být vždy rozšířený přístupový seznam. Příchozí přístupový seznam zakazuje provoz, který má podléhat inspekci CBAC. CBAC potom povolí jen ten návratový provoz, který patří k platné relaci, a bude pro něj v uvedeném přístupovém seznamu podle potřeby vytvářet dočasná povolení průchodu.

Druhá topologie, která je na *obrázku č.3*, je topologie, kde je CBAC konfigurováno nad **interním** rozhraním.



Obrázek č.3 – Konfigurace CBAC nad interním rozhraní
Cisco IOS Security Configuration Guide, str 275.

Popis:

- V této topologii je CBAC konfigurováno nad rozhraním Ethernel 0. Externí provoz má zde povolné využívání služeb z demilitarizované zóny (DMZ), nicméně nadále je externí provoz blokován v přístupu do interní sítě, mimo ten, který je součástí komunikační relace inicializované v interní síti.

Pokud je nad interním rozhraním definován příchozí (do rozhraní z internetu) přístupový seznam, může tento seznam povolovat příchozí síťový provoz, který bude podléhat kontrole CBAC, pokud by provoz povolen nebyl, nepodléhal by inspekci CBAC a pakety by byly jednoduše zahozeny.

Odchozím přístupovým seznamem nad interním rozhraním musí být vždy rozšířený přístupový seznam. Veškerý síťový provoz, spadající pod inspekci CBAC, musí tento příchozí přístupový seznam zamítat, protože CBAC bude povolovat jen ten návratový provoz, který patří k platné, stávající relaci, a bude pro něj v uvedeném přístupovém seznamu podle potřeby vytvářet dočasná povolení průchodu.

Konfigurace globálních časových limitů a prahových hodnot
Časové limity a prahové hodnoty stanovují v CBAC dobu, po kterou se o relacích budou udržovat stavové informace, a okamžiky zahození relací, které se nepodaří plně ustavit. Časové limity a prahové hodnoty platí globálně pro všechny relace.

V následující tabulce jsou běžné příkazy používané pro správu stavu relací s popisem a implicitními hodnotami.

Příkaz	Popis	Implicitní hodnota
ip inspect tcp syswait-time sekundy	Doba, po kterou software čeká u TCP relace k navázaní spojení než tuto relaci zahodí	**30** sekund
ip inspect tcp finwait-time sekund	Doba, po kterou bude relace TCP udržována jako aktivní i přes detekovanou výměnu paketu FIN.	**5** sekund
ip inspect tcp idle-time sekund	Doba po kterou bude relace TCP udržována i bez jakékoli aktivity (časový limit nečinnosti TCP)	**3600** sekund
ip inspect udp idle-time sekund	Doba po kterou bude relace UDP udržována i bez jakékoli aktivity (časový limit nečinnosti UDP)	**30** sekund
ip inspect dns-timeout sekund	Doba, po kterou bude relace vyhledávání názvů DNS udržována i bez jakékoli aktivity.	**5** sekund
ip inspect max-incomplete high počet	Počet existujících pootevřených relací, po jehož dosažení začne software polootevřené relace odstraňovat. Jedná se o obranu proti útoku odepření služeb (DoS)	**500** polootevřených
ip inspect max-incomplete low počet	Počet existujících pootevřených relací, po jehož dosažení přestane software polootevřené relace dále odstraňovat.	**400** polootevřených
Ip inspect tcp max-incomplete host počet **block-time** sekund	Počet existujících polootevřených relací TCP se stejnou cílovou adresou, po jehož dosažení začne software polootevřené relace se stejnou cílovou adresou odstraňovat. Způsob odstraňování polootevřených relací při překročení prahové hodnoty max-incomplete host se v CBAC liší podle toho, jestli je časový limit block-time roven nule, nebo je definován jako nenulové kladné číslo. Pokud je hodnota block-time rovna nule, odstraňuje CBAC s každým novým požadavkem spojení k danému hostiteli vždy nejstarší existující polootevřené relace ke stejnému hostiteli a průchod paketů SYN povoluje; jestliže je hodnota block-time ostře větší než nula, odstraní CBAC všechny existující polootevřené relace k danému hostiteli a poté všechny nové požadavky spojení blokuje. Toto blokování nových požadavků spojení trvá až do doby vypršení časového limitu blok-time	**50** existujících polootevřených relací TCP, **0** sekund, interval od **1 do 250**

Cisco IOS Firewall Intrusion Detection Systém

Hlavní vlastností Cisco IOS Firewall IDS je podpora technologie pro detekci nežádoucího pronikání (intrusion detection technology) pro střední a špičkové routry. Cisco IOS Firewall IDS je ideální pro jakoukoliv síť a speciálně pro místa, kde je router umístěn mezi jednotlivými segmenty sítě, mezi kterými je požadována zvýšená bezpečnost. Může také chránit internetové a intranetové spojení, u kterých je nařízená zvýšená bezpečnost, nebo připojení pobočky k hlavnímu sídlu společnosti nebo Internetu.

Detekční systém rozpoznává 59 nejběžnějších typů útoků pomocí signatur sloužících k detekování modelů podezřelého provozu v síti. Signatury typu útoku zahrnuté v Cisco IOS Firewall byly vybrány z širokého seznamu typických vzorů typů průniků. Signatury reprezentují vážné porušení bezpečnosti, nejběžnější síťové útoky a sběr dat skenováním. Popis Cisco IOS Firewall IDS signatur bude v další části této práce.

Jinými slovy Cisco IOS Firewall IDS je přímý detektor nežádoucího vnikání, sleduje pakety jak prochází přes router, každý skenuje a porovnává s IDS signaturami. Když detekuje podezřelou aktivitu, zareaguje dřív než může být narušena bezpečnost sítě. Událost uloží do logu pomocí syslog nebo Cisco Secure Intrusion Detection System pomocí protokolu Post Office. Síťový administrátor může nakonfigurovat IDS systém k výběru příslušné reakce na různé hrozby:

- Pošle výstrahu na syslog server nebo na Cisco Secure IDS Director (centrální řídicí rozhraní)
- Zahodí paket
- Resetuje TCP spojení

Pokud bezpečnost vyžaduje obě vlastnosti firewallu, ať už IDS nebo CBAC, mohou tyto vlastnosti běžet nezávisle na sobě a na různých rozhraních routeru.

Cisco Secure Intrusion Destection systém

Cisco Secure IDS (známy také jako NetRanger) je robustní, real-time, detekční systém pro odhalování, oznamování a přerušení neautorizovaných aktivit v síti. Cisco Secure IDS je plně kompatibilní s Cisco IOS Firewallem.

Cisco Secure IDS se skládá z těchto komponent:

- Sensor
- Director
- Post Office

Cisco Secure IDS Sensor jsou vysokorychlostní síťové aplikace analyzující obsah a kontext jednotlivých paketů rozhodující zda je provoz autorizován. Když se proud síťových dat jeví jako neautorizovaný nebo podezřele, například jako SATAN attack, ping sweep a podobné, Cisco Secure IDS Sensor může detekovat v reálném čase porušení bezpečnosti, rozeslat výstrahy k Cisco Secure IDS Direktor a patřičně reagovat.

Cisco Secure IDS Director je výkonný , softwarově založený řídící systém, který centrálně monitoruje aktivity více Cisco Secure IDS Sensors umístěných na lokálních nebo odlehlých síťových segmentech.

Cisco Secure IDS Post Office je komunikační protokol, který umožňuje Cisco Secure IDS službám a hostitelům vzájemnou komunikaci.

Uživatelé Cisco Secure IDS mohou rozšířit Cisco IOS Firewall IDS signatury k doplnění jejich existujících IDS systémů. Toto umožňuje rozšířit IDS v oblasti, kterou nemusí Cisco Secure IDS Sensor podporovat. Cisco IOS Firewall IDS signatury mohou být vyvíjeny vedle nebo nezávisle na ostatních vlastnostech Cisco IOS Firewallu.

Funkční popis Cisco IOS Firewallu

Cisco IOS Firewall IDS vystupuje jako přímý detektor vniknutí sledující pakety procházející rozhraními routeru zda jsou ve správném tvaru. Když paket, nebo řada paketů v toku souhlasí se signaturami, Cisco IOS Firewall IDS může provést následující nakonfigurovatelné akce:

- **Alarm** - Pošle alarm na syslog serveru nebo Cisco Secure IDS Director
- **Drop** - Zahodí pakety
- **Reset** - Resetuje TCP spojení

Následuje popis procesu konfigurace prověřování paketů pomocí Cisco IOS Firewall IDS:

- Vytvoříte kontrolní pravidlo, které specifikuje signatury, které mohou být použity na posílané pakety a akce, které se provedou, když je nalezena shoda. Prověřující pravidla mohou používat na pakety informační a útočné signatury (podrobněji v následující podkapitole). Jejich seznam může obsahovat jednu, všechny nebo jakýkoliv počet signatur.
- Použijete pravidlo na rozhraní routeru, specifikujete směr toku paketů (*in* nebo *out*).
- Když je pravidlo použito na příchozí směr rozhraní, pakety procházející rozhraním jsou kontrolovány před průchodem ACL (aby je nemohl ACL vyřadit). Toto umožní administrátory upozornit na útok nebo na nekalé aktivity i když by router normálně požadavek odfiltroval.
- Když je kontrolní pravidlo použito na odchozí směr na rozhraní, pakety jsou nejprve kontrolovány příchozích ACL po jejich vstupu na router z jiného rozhraní. V tomto případě, příchozí ACL jiného rozhraní může vyřadit pakety před jejich zkontrolováním Cisco IOS Firewall IDS. To může mít za následek, že Cisco IOS Firewall IDS neupozorní na útok, přestože útok byl již zmařen.
- Pakety procházející přes rozhraní, které provádí kontroly, jsou prověřovány sérií modulů, začínající s IP následované buďto ICMP, TCP, nebo UDP a nakonec aplikační vrstvou.
- Když je v modulu nalezena shoda se signaturou, nastanou následující uživatelem definované akce:
  - Když je vyvolaná akce **alarm**, potom modul dokončí kontrolu, pošle alarm a podstoupí paket dalšímu modulu.
  - V případě akce **drop**, je paket zahozen a neposílá se do dalšího modulu.

– V případě akce **reset**, se paket přepošle do dalšího modulu a je poslán paket s nastaveným reset flag oběma účastníkům spojení.

Poznámka
Je doporučeno používat **drop** a **reset** společně. Když je nalezeno více shod se signaturami v jednou modulu, pouze první nález vyvolá akci. Další nálezy v ostatních modulech také vyvolají akci, ale pouze jedinou za každý modul.

Popis signatur

Následuje popis signatur umístěných v seznamu Cisco IOS Firewall IDS. Signatury popisují vzory zneužití v síťovém provozu. V Cisco IOS Firewall IDS jsou signatury rozděleny do těchto čtyř skupin:

- Info Atomic
- Info Compound
- Attack Atomic
- Attack Compound

Info signatura detekuje information-gathering (shromáždění dat) aktivitu, jako je port sweep.

Attack signatura detekuje útok směřovaný do chráněné sítě, jako je odmítnutí služby nebo provedení neplatného příkazu během FTP relace.

Info a attack signatury můžou být buďto atomické nebo složené signatury. Atomické signatury můžou odhalit typy jednoduché jako pokusy přístupu ke konkrétnímu portu na konkrétním hostiteli. Složené signatury můžou odhalit komplexní útoky, jako je sekvence příkazů distribuovaných přes rozmanité hostitele v delších časových úsecích. Signatury pronikání zahrnuté v Cisco IOS Firewall byly vybrány z širokého spektra signatur průniků a nežádoucího vniknutí jako reprezentanté nejběžnějších síťových útoků a skenů pro shromaždování dat. Seznam všech 59 signatur obsažených v Cisco Secure IDS Network Security Databáze obsahující id, jméno, typ a popis je k nahlédnutí na webu Cisco, konkrétně http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/scfids.htm.

Konfigurace Cisco IOS Firewall IDS

V následujících tabulkách jsou uvedené příkazy sloužící ke konfiguraci Cisco IOS Firewall IDS. Jednotlivé části jsou označeny podle toho, zda jsou příkazy vyžadovány nebo zda jsou volitelné.
Prvním krokem je inicializace Post Office, tato část je vyžadována. Následujícím krokem je inicializace Cisco IOS Firewall IDS, která je také povinná. Poslední části je ověření konfigurace Cisco IOS Firewall IDS, která je volitelná

Inicializace Post Office

(vyžadována)

	Příkaz	Popis
Krok 1	Router(config)# **ip ips notify nr-director** Router(config)#**ip ips notify log**	Zaslání oznámení (alarm) buď Cisco Secure IDS Directoru nebo syslog serveru nebo oběma. Když se má poslat alarm Cisco Secure IDS Directoru, je užito klíčové slovo **nr-director**, pokud se má poslat alarm syslog serveru, je užito klíčové slovo **log**.
Krok 2	Router(config)# **logging console info**	Zobrazení zpráv syslogu na konzoli, pokud jsou posílány alarmy do syslogu.
Krok 3	Router(config)# **exit**	Opuštění globálního konfiguračního režimu.
Krok 4	Router# **write memory**	Uložení konfigurace.
Krok 5	Router# **reload**	Reloadovaní routeru.

Inicializace Cisco IOS Firewall IDS

(vyžadována)

Pro konfigurování ips pravidel, je potřeba použít následující příkazy v globálním konfiguračním režimu.

	Příkaz	Popis
Krok 1	Router(config)# **ip ips info** {**action** [**alarm**] [**drop**] [**reset**]} Router(config)# **ip ips attack** {**action** [**alarm**] [**drop**] [**reset**]}	Nastavení implicitní akcí pro info a attack signatury. Oba typy signatur mohou mít žádnou nebo všechny následující akce: alarm, drop a reset. Implicitní akce je **alarm.**
Krok 2	Router(config)# **ip ips name** *audit_name* {**info** | **attack**} [**list** *standard_acl*] [**action** [**alarm**] [**drop**] [**reset**]]	Vytvoření ips pravidel, kde *audit_name* je uživatelem definované jméno pravidel např.: **ip ips name** *audit_name* **info** (vytvoření pravidla pro info signatury) **ip ips name** *audit_name* **attack** (vytvoření pravidla pro attack signatury) Implicitní akce je **alarm**. Můžete také použit **ip ips name** příkaz pro připojení access control listů k ips pravidlům pro odfiltrování zdrojů

		nesprávných poplachů. *standard_acl* je číslo reprezentující access control list (ACL). Pokud je ACL přiřazen k ips pravidlu, musí být ACL definován také: **ip ips name** *audi_name* {**info**|**attack**} **list** *acl_list.* V následujícím příkladě je ACL 99 přiřazen k ips pravidlu INFO **ip ips name** INFO **info list** 99 **access-list** 99 **deny** 10.1.1.0 0.0.0.255 **access-list** 99 **permit any**
Krok 3	Router(config)# **ip ips signature** *signature-number* {**disable** | **list** *acl_list*}	Zakázaní konkrétní signatury. Zakázané signatury nejsou zahrnuty v ips pravidlech. **ip ips signature** *signature-number* **disable** Ke znovuzaktivování dříve zakázaných signatur se používá příkaz **no ip ips signature** *signature-number* **disable** kde *signature-number* je číslo zakázaného ips pravidla. Může se také použít příkaz **ip ips signature list** pro aplikováni signatury pro odfiltrování zdrojů nesprávných poplachů. *signature-number je* číslo signatury, a *acl_list* je číslo reprezentující ACL: **ip ips signature** *signature-number* **list** *acl_list* V následujícím příkladě je ACL 35 přiřazen k signatuře 1234: **ip ips signature** 1234 **list** 35 **access-list** 35 **deny** 10.1.1.0 0.0.0.255 **access-list** 35 **permit any**
Krok 4	Router(config-if)# **interface interface-number**	Vstup do konfiguračního režimu rozhraní.
Krok 5	Router(config-if)# **ip ips** *audit_name* {in | out}	Aplikování ips pravidla na rozhraní. V tomto příkazu *audit_name* je existující jméno ips pravidla a kontrola (směr) je buďto dovnitř (**in**) nebo ven(**out**).
Krok 6	Router(config-if)# **exit**	Opuštění konfiguračního režimu rozhraní.

Krok 7	Router(config)# **exit**	Opuštění globálního konfiguračního režimu.

Ověřování konfigurace Cisco IOS Firewall IDS

Pro ověřování Cisco IOS Firewallu IDS nakonfigurovaných vlastností slouží příkaz
show ip ips configuration

Př.:

ids2611# **show ip ips configuration**

Event notification through syslog is enabled
-stav hlášení událostí na syslog
Event notification through IDS Director is enabled
-stav hlášení událostí na ISD Director
Default action(s) for info signatures is alarm
-standardní akce pro info signatury
Default action(s) for attack signatures is alarm drop reset
-standardní akce pro attack signatury
PostOffice:HostID:55 OrgID:123 Msg dropped:0
:Curr Event Buf Size:100 Configured:100
HID:14 OID:123 S:1 A:2 H:82 HA:49 DA:0 R:0 Q:0
ID:1 Dest:10.1.1.99:45000 Loc:172.16.58.99:45000 T:5 S:ESTAB *
-nastavení protokolu IDS Post Office
Audit Rule Configuration
-výpis jednotlivých pravidel
Audit name AUDIT.1
-jméno pravidla AUDIT.1
info actions alarm
-provedení akce alarm při nalezení info signatury
attack actions alarm drop reset
-provedení akcí alarm, drop a reset při nalezení attack signatury

Pro ověřování rozhraní které obsahují kontrolní pravidla slouží příkaz
show ip ips interface

Př.:

ids2611# **show ip ips interface**

Interface Configuration
Interface Ethernet0
-nastavení IDS na rozhraní Ethernet0
Inbound IDS audit rule is AUDIT.1
-vstupní pravidlo na rozhraní Eth0 (v tomto případě AUDIT.1)
info actions alarm
-výpis nastavení pravidla AUDIT.1 pro info signatury
attack actions alarm drop reset
- výpis nastavení pravidla AUDIT.1 pro attack signatury

Outgoing IDS audit rule is not set
-výstupní pravidlo (v tomto případě není nastaveno)
Interface Ethernet1
-nastavení IDS na rozhraní Ethernet1
Inbound IDS audit rule is AUDIT.1
-vstupní pravidlo na rozhraní Eth1 (v tomto případě AUDIT.1)
info actions alarm
-výpis nastavení pravidla AUDIT.1 pro info signatury
attack actions alarm drop reset
-výpis nastavení pravidla AUDIT.1 pro attack signatury
Outgoing IDS audit rule is not set
-výstupní pravidlo (v tomto případě není nastaveno)

Monitorování a údržba Cisco IOS Firewall IDS

Následující tabulka uvádí příkazy pro monitorování a údržbu Cisco IOS Firewall IDS

Příkaz	Popis
Router# **clear ip ips statistics**	Vynuluje statistiku analyzovaných paketů vedených na IDS Director.
Router# **show ip ips statistics**	Zobrazení počtu prověřených paketů a počtu zaslaných alarmů a dalších informací

Příklad výstupu po aplikování příkazu **show ip audit statistics:**

Signature audit statistics [process switch:fast switch]
-výpis statistik kontrol podle jednotlivých signatur
signature 2000 packets audited: [0:2]
signature 2001 packets audited: [9:9]
signature 2004 packets audited: [0:2]
signature 3151 packets audited: [0:12]
Interfaces configured for audit 2
-počet rozhraní, na kterých je aktivní IDS
Session creations since subsystem startup or last reset 11
-počet spojení vytvořených od posledního startu nebo resetu IDS
Current session counts (estab/half-open/terminating) [0:0:0]
-počet aktuálních spojení (založené, jednostraně otevřené, přerušené)
Maxever session counts (estab/half-open/terminating) [2:1:0]
-maximální počet spojení (založené, jednostraně otevřené, přerušené)
Last session created 19:18:27
-čas poslední relace
Last statistic reset never
-čas posledního resetu (vymazání) statistik

Příklady konfigurace

V této části ukážeme ukázky typické konfigurace následujících situací:

- Základní nastavení Cisco IOS IDS
- Přidání ACL do kontrolních pravidel
- Vyřazení signatur
- Přidání ACL do signatur
- Použití více různých kontrolních pravidel

Základní nastavení Cisco IOS IDS

V následujícím příkladě je inicializováno Cisco IOS IDS. Všimněte si , že pravidlo AUDIT.1 bude používat obojí, jak info tak attack signatury:

```
ip ips notify nr-director
```
-zapisování událostí do IDS Directoru
```
ip ips notify log
```
-zapisování událostí do syslogu routeru

```
ip ips name AUDIT.1 info action alarm
```
-vytvoření a nastavení kontrolního pravidla AUDIT.1 pro info signatury
-jméno kontrolního pravidla: AUDIT.1
-akce při zjištění info signatury: alarm
```
ip ips name AUDIT.1 attack action alarm drop reset
```
-vytvoření a nastavení kontrolního pravidla AUDIT.1 pro attack signatury
-jméno kontrolního pravidla: AUDIT.1
-akce při zjištění attack signatury: alarm, drop, reset

```
interface e0
```
-nastavení rozhraní ethetnet0
```
ip address 10.1.1.1 255.255.255.0
```
-nastavení ip adresy
```
ip ips AUDIT.1 in
```
-zapnutí kontroly IDS na rozhraní eth0 podle pravidla AUDIT.1

```
interface e1
```
-nastavení rozhraní ethernet1
```
ip address 172.16.57.1 255.255.255.0
```
-nastavení ip adresy
```
ip ips AUDIT.1 in
```
-zapnutí kontroly IDS na rozhraní eth1 podle pravidla AUDIT.1

Přidání ACL do kontrolních pravidel

V následujícím příkladě je do kontrolního pravidla přidáno ACL. Díky kterému si můžeme určit, které pakety (z jednotlivých adres) budou kontrolovány a které ne. V našem případě pakety přicházející z adresy 172.16.57.4 kontrolovány IDS nebudou.

```
ip ips notify nr-director
ip ips notify log
```
-zapisování událostí do syslogu routeru a IDS Directoru

```
ip ips name AUDIT.1 info list 90 action alarm
```
-nastavení kontrolního pravidla AUDIT.1 pro info signatury
-jméno kontrolního pravidla: AUDIT.1
-použití ACL pro výběr kontrolovaných paketů : klíčové slovo list a jméno ACL
-akce při zjištění info signatury: alarm

```
ip ips name AUDIT.1 attack list 90 action alarm drop reset
```
-nastavení kontrolního pravidla AUDIT.1 pro attack signatury
-jméno kontrolního pravidla: AUDIT.1
-použití ACL pro výběr kontrolovaných paketů : klíčové slovo list a jméno ACL
-akce při zjištění attack signatury: alarm, drop, reset

```
interface e0
```
-nastavení rozhraní Eth0
```
ip address 10.1.1.1 255.255.255.0
ip ips AUDIT.1 in
```

```
interface e1
```
-nastavení rozhraní Eth1
```
ip address 172.16.57.1 255.255.255.0
ip ips AUDIT.1 in
```

```
access-list 90 deny 172.16.57.4
```
-odfiltrování provozu z ip adresy 172.16.57.4
```
access-list 90 permit any
```
-ostatní provoz povolen

Vyřazení signatur

Bezpečnostní administrátor si všimnul, že router generuje mnoho chybných výsledků pro signatury 1234, 2345 a 3456. Administrátor ví, že na síti je aplikace, která zapříčiňuje vyvolání signatury 1234 a není to aplikace, která zvyšuje bezpečnostní riziko. Signaturu můžeme vyřadit jako je zobrazeno v následujícím příkladě:

```
ip ips notify nr-director
ip ips notify log
```
-zapisování událostí do syslogu routeru a IDS Directoru

```
ip ips signature 1234 disable
```
-vypnutí kontroly IDS na signaturu 1234

```
ip ips name AUDIT.1 info action alarm
```
-nastavení kontrolního pravidla AUDIT.1 pro info signatury
```
ip ips name AUDIT.1 attack action alarm drop reset
```
-nastavení kontrolního pravidla AUDIT.1 pro attack signatury

```
interface e0
```
-nastavení rozhraní Eth0
```
ip address 10.1.1.1 255.255.255.0
ip ips AUDIT.1 in
```

Přidání ACL do signatur

Po větším zkoumání bezpečnostní administrátor objeví, že chybné výsledky pro signatury 4050 a 1206 jsou zapříčiněny určitou aplikací na 10.1.1.3 a 10.1.1.4. Přidáním ACL, která zabrání kontrole signatur 4050 a 1206 z výše uvedených ip adres, se zastaví vytváření chybných poplachů, jak je znázorněno v příkladě:

```
ip audit notify nr-director
ip audit notify log
```
-zapisování událostí do syslogu routeru a IDS Directoru

```
ip ips signature 4050 list 91
```
-vypnutí kontroly IDS na signaturu 4050 z ip adres dle ACL
```
ip ips signature 1206 list 91
```
-vypnutí kontroly IDS na signaturu 1206 z ip adres dle ACL

```
ip ips name AUDIT.1 info action alarm
```
-nastavení kontrolního pravidla AUDIT.1 pro info signatury
```
ip ips name AUDIT.1 attack action alarm drop reset
```
-nastavení kontrolního pravidla AUDIT.1 pro attack signatur

```
interface e0
```
-nastavení rozhraní Eth0
```
ip address 10.1.1.1 255.255.255.0
ip ips AUDIT.1 in

access-list 91 deny host 10.1.1.3
```
-odfiltrování provozu z ip adresy 10.1.1.3
```
access-list 91 deny host 10.1.1.4
```
- odfiltrování provozu z ip adresy 10.1.1.4
```
access-list 91 permit any
```
-ostatní provoz povolen

Použití více různých kontrolních pravidel

Společnost se nyní reorganizovala a má na síti 10.1.1.0 umístěné pouze spolehlivé lidi. Zaměstnanci dokončená práce na této síti nesmí být narušena s Cisco IOS IDS, takže attack signatury v AUDIT.1 pravidlu vyvolají pouze alarm. Pro spojení vytvořené mimo tuto síť, budou nalezené attack signatury řešeny standardním způsobem: poslání upozornění (alarm), vypuštění paketu (drop) a reset TCP spojení (reset). Nakonfigurování dvou různých kontrolních pravidel a jejich použití na různá ethernetová rozhraní jak je naznačeno v následujícím příkladě:

```
ip ips notify nr-director
ip ips notify log
```
-zapisování událostí do syslogu routeru a IDS Directoru

```
ip ips name AUDIT.1 info action alarm
```
-vytvoření a nastavení kontrolního pravidla AUDIT.1 pro info signatury
-jméno kontrolního pravidla: AUDIT.1
-akce při zjištění info signatury: alarm
```
ip ips name AUDIT.1 attack action alarm
```
-vytvoření a nastavení kontrolního pravidla AUDIT.1 pro attack signatury

-jméno kontrolního pravidla: AUDIT.1
-akce při zjištění attack signatury: alarm

```
ip ips name AUDIT.2 info action alarm
```

-vytvoření a nastavení kontrolního pravidla AUDIT.2 pro info signatury
-jméno kontrolního pravidla: AUDIT.2
-akce při zjištění info signatury: alarm

```
ip ips name AUDIT.2 attack action alarm drop reset
```

-vytvoření a nastavení kontrolního pravidla AUDIT.2 pro attack signatury
-jméno kontrolního pravidla: AUDIT.2
-akce při zjištění attack signatury: alarm, drop, reset

```
interface e0
```

-nastavení rozhraní Eth0

```
ip address 10.1.1.1 255.255.255.0
```

-nastavení ip adresy na rozhraní eth0

```
ip ips AUDIT.1 in
```

-zapnutí kontroly IDS na rozhraní eth0 podle pravidla AUDIT.1

```
interface e1
```

-nastavení rozhraní Eth1

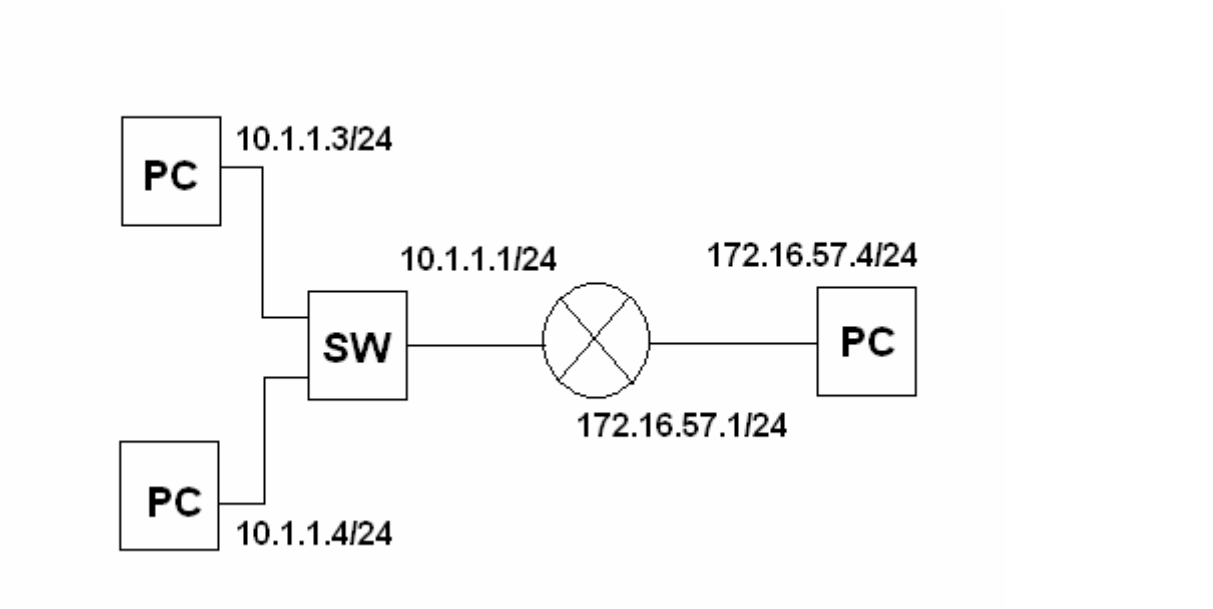
```
ip address 172.16.57.1 255.255.255.0
```

-nastavení ip adresy na rozhraní eth1

```
ip ips AUDIT.2 in
```

-zapnutí kontroly IDS na rozhraní eth1 podle pravidla AUDIT.2

Výše uvedené příklady konfigurace byly převzaty z webových stránek www.cisco.com, upraveny a otestovány ve školní laboratoři Cisco na routeru Cisco 2800, který byl zapojen dle následující topologie:



Po sestavení sítě a nakonfigurování routeru (viz jednotlivé ukázky konfigurace) jsme na připojených PC (s OS Linux) rozběhli utilitu IDSWakeUp. Tato utilita složí k testování a ověření IDS systémů a je volně dosažitelná na internetu na adrese http://www.hsc.fr/ressources/outils/idswakeup/index.html.en . Utilita provádí různé druhy útoků na zadanou cílovou ip adresu.

Spuštění IDSWakeUp: `idswakeup <zdrojová adresa> <cílová adresa>`

Pro lepší názornost jsme si na routeru nastavili zobrazování zpráv o útoku nejen do syslogu, ale také na konzoli (pomocí příkazu logging console info). Jako cílové ip adresy jsme nastavovali jak adresy rozhraní routeru tak adresy ostatních PC v síti. Sledovali jsme zda opravdu při použití ACL přestane router na útoky reagovat, či při vyřazení některých signatur se opravdu přestanou zobrazovat varování o útoku pomocí těchto signatur.

Po odzkoušení všech předešlých konfigurací a různých možných útoků jsme si ověřili, že opravdu se router s IDS choval přesně tak jak bychom od něj čekali a požadovali.

Provádění útoků na IDS pomocí IDSWakeUp

Následuje ukázka výpisu provedených útoků. Jedná se o běžné útoky na služby ftp, www, smtp, dos nebo telnet pomocí protokolů icmp, tcp, udp a podobně.

```
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
-  IDSwakeup : false positive generator              -
-  Stephane Aubert                                   -
-  Hervé Schauer Consultants (c) 2000                -
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

  src_addr:10.1.1.3  dst_addr:10.1.1.1  nb:1   ttl:3

  sending : teardrop ...
  sending : land ...
  sending : get_phf ...
  sending : bind_version ...
  sending : get_phf_syn_ack_get ...
  sending : ping_of_death ...
  sending : syndrop ...
  sending : newtear ...
  sending : X11 ...
  sending : SMBnegprot ...
  sending : smtp_expn_root ...
  sending : finger_redirect ...
  sending : ftp_cwd_root ...
  sending : ftp_port ...
  sending : trin00_pong ...
  sending : back_orifice ...
  sending : msadcs ...
          10.1.1.3 -> 10.1.1.1 80/tcp  GET /msadc/msadcs.dll HTTP/1.0
  sending : www_frag ...
          10.1.1.3 -> 10.1.1.1 80/fragmented-tcp  GET /..... HTTP/1.0
          10.1.1.3 -> 10.1.1.1 80/fragmented-tcp  GET /
          AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
          AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
          AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAA/../cgi-bin/phf HTTP/1.0

sending : www_bestof ...

10.1.1.3 -> 10.1.1.1 80/tcp GET / HTTP/1.0
10.1.1.3 -> 10.1.1.1 80/tcp GET //////// HTTP/1.0
10.1.1.3 -> 10.1.1.1 80/tcp HEAD / HTTP/1.0
10.1.1.3 -> 10.1.1.1 80/tcp HEAD/./
10.1.1.3 -> 10.1.1.1 80/tcp /cgi-bin\\handler
10.1.1.3 -> 10.1.1.1 80/tcp /cgi-bin\\webdist.cgi
10.1.1.3 -> 10.1.1.1 80/tcp /mlog.phtml
10.1.1.3 -> 10.1.1.1 80/tcp /mylog.phtml
10.1.1.3 -> 10.1.1.1 80/tcp /cfide\\administrator\\startstop.html
10.1.1.3 -> 10.1.1.1 80/tcp /cfappman\\index.cfm
10.1.1.3 -> 10.1.1.1 80/tcp /mall_log_files\\order.log
10.1.1.3 -> 10.1.1.1 80/tcp /admin_files\\order.log
10.1.1.3 -> 10.1.1.1 80/tcp /cgi-bin\\wrap
10.1.1.3 -> 10.1.1.1 80/tcp GET /cgi-bin/ph%66 HTTP/1.0
10.1.1.3 -> 10.1.1.1 80/tcp GET /sahsc.lnk HTTP/1.0
10.1.1.3 -> 10.1.1.1 80/tcp GET /sahsc.bat HTTP/1.0
10.1.1.3 -> 10.1.1.1 80/tcp GET /sahsc.url HTTP/1.0
10.1.1.3 -> 10.1.1.1 80/tcp GET /sahsc.ida HTTP/1.0
10.1.1.3 -> 10.1.1.1 80/tcp GET /default.asp::$DATA HTTP/1.0
10.1.1.3 -> 10.1.1.1 80/tcp GET / HTTP/1.0
10.1.1.3 -> 10.1.1.1 80/tcp PUT /scripts/cmd.exe HTTP/1.0
10.1.1.3 -> 10.1.1.1 80/tcp GET /scripts/cmd.exe HTTP/1.0
10.1.1.3 -> 10.1.1.1 80/tcp BAD /scripts/cmd.exe HTTP/1.0
10.1.1.3 -> 10.1.1.1 80/tcp GET /_vti_pvt/administrators.pwd HTTP/1.0
10.1.1.3 -> 10.1.1.1 80/tcp GET /cgi-bin/handler HTTP/1.0
10.1.1.3 -> 10.1.1.1 80/tcp GET /../../../../../../etc/passwd HTTP/1.0
10.1.1.3 -> 10.1.1.1 80/tcp GET /cgi-bin/perl.exe HTTP/1.0
10.1.1.3 -> 10.1.1.1 80/tcp GET /scripts/tools/newdsn.exe HTTP/1.0
10.1.1.3 -> 10.1.1.1 80/tcp GET /search97.vts HTTP/1.0
10.1.1.3 -> 10.1.1.1 80/tcp GET /IISADMIN HTTP/1.0

sending : ddos_bestof ...

10.1.1.3 -> 10.1.1.1 15104/tcp -S
10.1.1.3 -> 10.1.1.1 1712/tcp -PA >
10.1.1.3 -> 10.1.1.1 12754/tcp -PA >
10.1.1.3 -> 10.1.1.1 10498/udp pong
10.1.1.3 -> 10.1.1.1 10498/udp ping
10.1.1.3 -> 10.1.1.1 10498/udp stream/
10.1.1.3 -> 10.1.1.1 6838/udp newserver
10.1.1.3 -> 10.1.1.1 27665/tcp killme
10.1.1.3 -> 10.1.1.1 31335/udp PONG
10.1.1.3 -> 10.1.1.1 1695/udp l44
10.1.1.3 -> 10.1.1.1 1624/udp *HELLO*
10.1.1.3 -> 10.1.1.1 27665/tcp gOrave
10.1.1.3 -> 10.1.1.1 20432/tcp
10.1.1.3 -> 10.1.1.1 18753/udp alive tijgu
10.1.1.3 -> 10.1.1.1 20433/udp alive
10.1.1.3 -> 10.1.1.1 1659/tcp -S --setseq 674711609

sending : ftp_bestof ...

10.1.1.3 -> 10.1.1.1 21/tcp PORT 127,0,0,1,0,23
10.1.1.3 -> 10.1.1.1 21/tcp PORT 10,6,6,6,0,23
10.1.1.3 -> 10.1.1.1 21/tcp PORT 127,0,0,1,255,510
10.1.1.3 -> 10.1.1.1 21/tcp passwd
10.1.1.3 -> 10.1.1.1 21/tcp site exec %p%p%p%p%p%p
10.1.1.3 -> 10.1.1.1 21/tcp SITE exec cat /etc/passwd ;-)
10.1.1.3 -> 10.1.1.1 21/tcp SYST /etc/passwd ;-)
10.1.1.3 -> 10.1.1.1 21/tcp SYST
10.1.1.3 -> 10.1.1.1 21/tcp CWD ~root

10.1.1.3 -> 10.1.1.1 21/tcp STOR |
10.1.1.3 -> 10.1.1.1 21/tcp RETR |
sending : telnet_bestof ...
10.1.1.3 -> 10.1.1.1 23/tcp ciscociscociscociscociscociscociscociscociscociscocisco
10.1.1.3 -> 10.1.1.1 23/tcp bof
10.1.1.3 -> 10.1.1.1 23/tcp IFS=/
10.1.1.3 -> 10.1.1.1 23/tcp su - root
10.1.1.3 -> 10.1.1.1 23/tcp su root
10.1.1.3 -> 10.1.1.1 23/tcp id; cat /etc/shadow
10.1.1.3 -> 10.1.1.1 23/tcp echo "+ +">.rhosts
10.1.1.3 -> 10.1.1.1 23/tcp resolv_host_conf
10.1.1.3 -> 10.1.1.1 23/tcp ld_preload
10.1.1.3 -> 10.1.1.1 23/tcp ld_library_pat
sending : rlogin_bestof ...
10.1.1.3 -> 10.1.1.1 513/tcp IFS=/
10.1.1.3 -> 10.1.1.1 513/tcp su - root
10.1.1.3 -> 10.1.1.1 513/tcp su root
10.1.1.3 -> 10.1.1.1 513/tcp id; cat /etc/shadow
10.1.1.3 -> 10.1.1.1 513/tcp echo "+ +">.rhosts
sending : tcpflag_bestof ...
10.1.1.3 -> 10.1.1.1 80/tcp -SF
10.1.1.3 -> 10.1.1.1 80/tcp -SR
10.1.1.3 -> 10.1.1.1 80/tcp
10.1.1.3 -> 10.1.1.1 80/tcp -A
10.1.1.3 -> 10.1.1.1 80/tcp -SFR
10.1.1.3 -> 10.1.1.1 80/tcp -SFARPXY
10.1.1.3 -> 10.1.1.1 80/tcp -SA
10.1.1.3 -> 10.1.1.1 80/tcp -SAFR
10.1.1.3 -> 10.1.1.1 80/tcp -XY
10.1.1.3 -> 10.1.1.1 1999/tcp -S
sending : icmp_bestof ...
10.1.1.3 -> 10.1.1.1 icmp type:0 code:0
10.1.1.3 -> 10.1.1.1 icmp type:0 code:0 Hi B0B !...
10.1.1.3 -> 10.1.1.1 icmp type:3 code:0
10.1.1.3 -> 10.1.1.1 icmp type:3 code:1
10.1.1.3 -> 10.1.1.1 icmp type:3 code:2
10.1.1.3 -> 10.1.1.1 icmp type:3 code:3
10.1.1.3 -> 10.1.1.1 icmp type:3 code:4
10.1.1.3 -> 10.1.1.1 icmp type:3 code:5
10.1.1.3 -> 10.1.1.1 icmp type:3 code:13
10.1.1.3 -> 10.1.1.1 icmp type:3 code:14
10.1.1.3 -> 10.1.1.1 icmp type:3 code:15
10.1.1.3 -> 10.1.1.1 icmp type:4 code:0
10.1.1.3 -> 10.1.1.1 icmp type:5 code:0
10.1.1.3 -> 10.1.1.1 icmp type:5 code:1
10.1.1.3 -> 10.1.1.1 icmp type:5 code:2
10.1.1.3 -> 10.1.1.1 icmp type:5 code:3
10.1.1.3 -> 10.1.1.1 icmp type:8 code:0
10.1.1.3 -> 10.1.1.1 icmp type:11 code:0
10.1.1.3 -> 10.1.1.1 icmp type:11 code:1
10.1.1.3 -> 10.1.1.1 icmp type:12 code:0
10.1.1.3 -> 10.1.1.1 icmp type:13 code:0
10.1.1.3 -> 10.1.1.1 icmp type:14 code:0
10.1.1.3 -> 10.1.1.1 icmp type:15 code:0
10.1.1.3 -> 10.1.1.1 icmp type:16 code:0
10.1.1.3 -> 10.1.1.1 icmp type:17 code:0
10.1.1.3 -> 10.1.1.1 icmp type:18 code:0
sending : smtp_bestof ...
10.1.1.3 -> 10.1.1.1 25/tcp rcpt to: bouncebounce
10.1.1.3 -> 10.1.1.1 25/tcp expn root

```
        10.1.1.3 -> 10.1.1.1 25/tcp  expn decode
        10.1.1.3 -> 10.1.1.1 25/tcp  debug
        10.1.1.3 -> 10.1.1.1 25/tcp  vrfy smtp
        10.1.1.3 -> 10.1.1.1 25/tcp  mail from: |
        10.1.1.3 -> 10.1.1.1 25/tcp  rcpt to: |
sending : misc_bestof ...
        10.1.1.3 -> 10.1.1.1 161/udp  public
        10.1.1.3 -> 10.1.1.1 161/udp  private
        10.1.1.3 -> 10.1.1.1 161/udp  all private
        10.1.1.3 -> 10.1.1.1 162/udp  trap trap trap ...
        10.1.1.3 -> 10.1.1.1 5631/tcp  ADMINISTRATOR
        10.1.1.3 -> 10.1.1.1 32771/tcp -S
        10.1.1.3 -> 10.1.1.1 6699/tcp  .mp3
        10.1.1.3 -> 10.1.1.1 8888/tcp  .mp3
        10.1.1.3 -> 10.1.1.1 7777/tcp  .mp3
        10.1.1.3 -> 10.1.1.1 6666/tcp  .mp3
        10.1.1.3 -> 10.1.1.1 5555/tcp  .mp3
        10.1.1.3 -> 10.1.1.1 4444/tcp  .mp3
        10.1.1.3 -> 10.1.1.1 8875/tcp  anon@napster.com
sending : dos_chargen ...
        10.1.1.3 -> 10.1.1.1 19/udp  hello
sending : dos_snork ...
        10.1.1.3 -> 10.1.1.1 135/udp  hi !...
sending : dos_syslog ...
        10.1.1.3 -> 10.1.1.1 514/udp  B0MB
```

Vyhodnocení útoků na routeru

Po spuštění utility IDSWakeUp, IDS začal okamžitě podle konfigurace zobrazovat hlášení o nekalé činnosti. Toto hlášení obsahuje datum a čas útoku, Typ signatury, se kterou se shoduje, tedy typ útoku, jeho textový popis a ip adresy, odkud a kam směřoval. Následuje krátká ukázka jak toto hlášení vypadalo:

```
*May 24 11:36:38.443: %IPS-4-SIGNATURE: Sig:1206 Subsig:0 Sev:2 Frag Too Small [10.1.1.3:58942 -> 10.1.1.1:17485]
*May 24 11:36:38.443: %IPS-4-SIGNATURE: Sig:4050 Subsig:0 Sev:3 UDP Bomb [10.1.1.3:58942 -> 10.1.1.1:17485]
*May 24 11:36:38.475: %IPS-4-SIGNATURE: Sig:1102 Subsig:0 Sev:5 Impossible IP packet [10.1.1.1:53 -> 10.1.1.1:1333]
*May 24 11:36:38.487: %IPS-4-SIGNATURE: Sig:4050 Subsig:0 Sev:3 UDP Bomb [10.1.1.3:1249 -> 10.1.1.1:53]
*May 24 11:36:38.507: %IPS-4-SIGNATURE: Sig:1206 Subsig:0 Sev:2 Frag Too Small [10.1.1.3:49925 -> 10.1.1.1:40935]
*May 24 11:36:38.511: %IPS-4-SIGNATURE: Sig:1206 Subsig:0 Sev:2 Frag Too Small [10.1.1.3:29936 -> 10.1.1.1:23775]
*May 24 11:36:38.511: %IPS-4-SIGNATURE: Sig:4050 Subsig:0 Sev:3 UDP Bomb [10.1.1.3:29936 -> 10.1.1.1:23775]
*May 24 11:36:38.571: %IPS-4-SIGNATURE: Sig:4050 Subsig:0 Sev:3 UDP Bomb [10.1.1.3:1249 -> 10.1.1.1:31335]
*May 24 11:36:38.575: %IPS-4-SIGNATURE: Sig:4050 Subsig:0 Sev:3 UDP Bomb [10.1.1.3:1249 -> 10.1.1.1:31337]
*May 24 11:36:38.659: %IPS-4-SIGNATURE: Sig:1206 Subsig:0 Sev:2 Frag Too Small [10.1.1.3:2714 -> 10.1.1.1:80]
*May 24 11:36:40.627: %IPS-4-SIGNATURE: Sig:4050 Subsig:0 Sev:3 UDP Bomb [10.1.1.3:1651 -> 10.1.1.1:10498]
*May 24 11:36:40.719: %IPS-4-SIGNATURE: Sig:4050 Subsig:0 Sev:3 UDP Bomb [10.1.1.3:1748 -> 10.1.1.1:10498]
*May 24 11:36:41.755: %IPS-4-SIGNATURE: Sig:4050 Subsig:0 Sev:3 UDP Bomb [10.1.1.3:1593 -> 10.1.1.1:10498]
*May 24 11:36:41.847: %IPS-4-SIGNATURE: Sig:4050 Subsig:0 Sev:3 UDP Bomb [10.1.1.3:1722 -> 10.1.1.1:6838]
*May 24 11:36:42.967: %IPS-4-SIGNATURE: Sig:4050 Subsig:0 Sev:3 UDP Bomb [10.1.1.3:1639 -> 10.1.1.1:31335]
*May 24 11:36:43.059: %IPS-4-SIGNATURE: Sig:4050 Subsig:0 Sev:3 UDP Bomb [10.1.1.3:31335 -> 10.1.1.1:1768]
*May 24 11:36:43.791: %IPS-4-SIGNATURE: Sig:4050 Subsig:0 Sev:3 UDP Bomb [10.1.1.3:1071 -> 158.196.147.15:53]
*May 24 11:36:44.095: %IPS-4-SIGNATURE: Sig:4050 Subsig:0 Sev:3 UDP Bomb [10.1.1.3:31335 -> 10.1.1.1:1773]
*May 24 11:36:45.187: %IPS-4-SIGNATURE: Sig:4050 Subsig:0 Sev:3 UDP Bomb [10.1.1.3:1638 -> 10.1.1.1:18753]
*May 24 11:36:45.279: %IPS-4-SIGNATURE: Sig:4050 Subsig:0 Sev:3 UDP Bomb [10.1.1.3:1691 -> 10.1.1.1:20433]
*May 24 11:36:47.899: %IPS-4-SIGNATURE: Sig:3041 Subsig:0 Sev:5 TCP SYN/FIN Packet [10.1.1.3:1705 -> 10.1.1.1:80]
*May 24 11:36:48.799: %IPS-4-SIGNATURE: Sig:4050 Subsig:0 Sev:3 UDP Bomb [10.1.1.3:1072 -> 158.196.149.9:53]
*May 24 11:36:49.975: %IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:5 TCP NULL Packet [10.1.1.3:1591 -> 10.1.1.1:80]
*May 24 11:36:50.107: %IPS-4-SIGNATURE: Sig:3041 Subsig:0 Sev:5 TCP SYN/FIN Packet [10.1.1.3:1765 -> 10.1.1.1:80]
*May 24 11:36:53.315: %IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:5 TCP NULL Packet [10.1.1.3:1777 -> 10.1.1.1:80]
*May 24 11:36:53.495: %IPS-4-SIGNATURE: Sig:2000 Subsig:0 Sev:2 ICMP Echo Rply [10.1.1.3:0 -> 10.1.1.1:0]
*May 24 11:36:54.527: %IPS-4-SIGNATURE: Sig:2000 Subsig:0 Sev:2 ICMP Echo Rply [10.1.1.3:0 -> 10.1.1.1:0]
*May 24 11:36:55.555: %IPS-4-SIGNATURE: Sig:2001 Subsig:0 Sev:2 ICMP Unreachable [10.1.1.3:0 -> 10.1.1.1:0]
```