

IDŹ DO

PRZYKŁADOWY ROZDZIAŁ



SPIS TREŚCI

KATALOG KSIĄŻEK

KATALOG ONLINE

ZAMÓW DRUKOWANY KATALOG

TWÓJ KOSZYK

DODAJ DO KOSZYKA

CENNIK I INFORMACJE

ZAMÓW INFORMACJE
O NOWOŚCIACH

ZAMÓW CENNIK

CZYTELNIA

FRAGMENTY KSIĄŻEK ONLINE

Wielka księga firewallei

Autor: pełna lista autorów – patrz w uwagach dodatkowych
Tłumaczenie: Sławomir Dzieniszewski, Marcin Jędrzyak,
Jan Ostrowski, Marek Pałczyński, Przemysław Steć.

Redakcja rozdziału 5. Radosław Sokół

ISBN: 83-7361-461-3

Tytuł oryginału: [Best Damn Firewall Book Period](#)

Format: B5, stron: 1376



Wszystko zaczęło się od list dostępu na routerach. Potem, niestety odkryto, że zabezpieczenia oferowane przez takie rozwiązania nie są zbyt skuteczne, co spowodowało wzrost liczby włamań do sieci. Pojawiły się więc firewalle – najpierw jako elementy pośredniczące, działające na poziomie aplikacji, potem – jako punkty kontrolne na granicach sieci komputerowych. Dzięki możliwościom firewallei możemy określić, które elementy sieci są godne zaufania, a które nie i odpowiednio filtrować dostęp do naszej sieci lokalnej.

Książka „Wielka księga firewallei” to przewodnik po najczęściej wykorzystywanych obecnie mechanizmach zapór sieciowych. Przedstawia podstawowe zagadnienia związane z bezpieczeństwem sieci komputerowych, opisuje podstawowe typy rozwiązań stosowanych w firewallach oraz wprowadza czytelnika w temat wykrywania włamań do sieci.

Oprócz niezbędnej dozy informacji teoretycznych książka zawiera ogromną porcję wiedzy praktycznej dotyczącej konfigurowania firewallei i routerów, projektowania i wdrażania sieci granicznych (DMZ), metod wykrywania włamań do sieci i usuwania ich skutków. „Wielka księga firewallei” zawiera wszystko, co trzeba wiedzieć o konfigurowaniu firewallei oraz wdrażaniu najbardziej zaawansowanych systemów wykrywania włamań.

- Bezpieczeństwo informacji
- Podstawowe pojęcia związane z firewallami
- Strefy DMZ i systemy detekcji włamań
- Firewalle dla systemów Linux i Solaris
- Firewalle PIX
- Firewalle Check Point NG i Nokia IP Series
- Serwer ISA
- Wykrywanie włamań za pomocą aplikacji Snort



Spis treści

| | | |
|--------------------|--|-----------|
| | Współautorka i redaktor merytoryczny | 17 |
| | Autorzy i konsultanci..... | 17 |
| | Przedmowa | 21 |
| Część I | Wprowadzenie do firewalli i problemów bezpieczeństwa w sieci | 23 |
| Rozdział 1. | Wprowadzenie do problemów bezpieczeństwa informacji | 25 |
| | Wprowadzenie | 25 |
| | Konsekwencje braku systemu bezpieczeństwa w dobie internetu..... | 26 |
| | Definiowanie bezpieczeństwa informacji | 29 |
| | Podstawowe pojęcia związane z bezpieczeństwem | 31 |
| | Wiedza to władza..... | 32 |
| | Myśl jak złodziej..... | 32 |
| | Blokowanie dróg, którymi można się włamać | 33 |
| | Rodzaje zagrożeń i ataków na system | 34 |
| | Fizyczne bezpieczeństwo..... | 34 |
| | Bezpieczeństwo sieciowe..... | 36 |
| | Motywacje włamywaczy | 37 |
| | Podstawowe kategorie rozwiązań stosowanych w systemach bezpieczeństwa..... | 40 |
| | Wracając do źródeł: standardowe porty TCP/UDP..... | 40 |
| | Klasyfikacja różnych typów ataków | 45 |
| | Polityki bezpieczeństwa..... | 57 |
| | Zapobieganie celowym naruszeniom systemu bezpieczeństwa od wewnątrz..... | 57 |
| | Ustalanie, kto powinien być odpowiedzialny za bezpieczeństwo sieci..... | 58 |
| | Ustalanie odpowiedzialności za przygotowanie planu i polityk bezpieczeństwa..... | 58 |
| | Projektowanie polityki bezpieczeństwa firmy | 59 |
| | Określanie naszych potrzeb w zakresie bezpieczeństwa..... | 65 |
| | Oficjalne klasyfikacje bezpieczeństwa..... | 68 |
| | Cele, które należy uwzględnić w planie bezpieczeństwa | 69 |
| | Tworzenie polityki bezpieczeństwa | 70 |
| | Edukowanie użytkowników sieci w zakresie bezpieczeństwa | 71 |
| | Ochrona infrastruktury systemu informatycznego | 74 |
| | Poprawianie systemu bezpieczeństwa..... | 74 |
| | Korzystanie z protokołu SSL i Secure Shell | 76 |
| | Testowanie systemu bezpieczeństwa | 77 |

| | | |
|--------------------|--|------------|
| | Inne rozwiązania sprzętowe wykorzystywane w systemach bezpieczeństwa | 79 |
| | Monitorowanie aktywności użytkowników w sieci | 79 |
| | Zapobieganie atakom z zewnątrz oraz nieautoryzowanym wejściom do systemu z zewnętrznych sieci | 81 |
| | Podsumowanie | 82 |
| Rozdział 2. | Podstawowe pojęcia związane z firewallami | 83 |
| | Wprowadzenie | 83 |
| | Definicja firewalla..... | 83 |
| | Typy firewalli | 85 |
| | Sieci i firewalle | 87 |
| | Interfejsy firewalli: wewnętrzny, zewnętrzny i strefy DMZ | 88 |
| | Polityki firewalli | 91 |
| | Tłumaczenie adresów | 91 |
| | Wirtualne sieci prywatne | 94 |
| | Popularne firewalle | 96 |
| | Firewalle sprzętowe | 98 |
| | Firewalle programowe | 100 |
| | Podsumowanie | 101 |
| Rozdział 3. | Pojęcie, konstrukcja i zasady projektowania strefy DMZ..... | 103 |
| | Wprowadzenie | 103 |
| | Podstawy stref DMZ | 104 |
| | Podstawowe przykłady stref DMZ | 107 |
| | Pojęcia związane z przepływem danych | 112 |
| | Sieci ze strefami DMZ a sieci bez nich..... | 115 |
| | Podstawowe zasady projektowania stref zdemilitaryzowanych | 116 |
| | Dlaczego faza projektowania jest tak ważna?..... | 117 |
| | Projektowanie zabezpieczeń dla potrzeb bezpośredniej transmisji danych między hostami w sieci..... | 120 |
| | Podstawowe informacje o przepływie danych w sieci i protokołach transmisji danych ... | 121 |
| | Projektowanie ochrony w odpowiedzi na naturalne słabości protokołów TCP/IPv4 ... | 122 |
| | Publiczne i prywatne adresy IP..... | 123 |
| | Porty | 123 |
| | Wykorzystanie firewalli do ochrony zasobów sieciowych | 124 |
| | Przepływ danych a zagrożenia dla systemu bezpieczeństwa | 127 |
| | Zagrożenia w szczególnych zastosowaniach stref DMZ | 131 |
| | Połączenia z partnerami biznesowymi | 131 |
| | Witryny WWW i FTP..... | 132 |
| | Usługi e-mail | 132 |
| | Zaawansowane strategie projektowania stref DMZ | 133 |
| | Zaawansowane zagadnienia związane z projektowaniem stref DMZ..... | 133 |
| | Dostępność strefy zdemilitaryzowanej i przejmowanie przez firewall funkcji innego firewalla | 136 |
| | Podsumowanie | 140 |
| Rozdział 4. | Wprowadzenie do systemów wykrywania włamań | 141 |
| | Wprowadzenie | 141 |
| | Na czym polega wykrywanie włamań?..... | 142 |
| | Sieciowe systemy IDS | 144 |
| | Systemy IDS dla hostów..... | 145 |
| | Rozproszone systemy IDS | 146 |

| | |
|--|-----|
| Jak rozpoznać włamanie?..... | 147 |
| Dlaczego systemy wykrywania włamań są tak ważne? | 148 |
| Dlaczego atakujący interesują się właśnie mną?..... | 149 |
| Jak dopasować system IDS do naszego planu bezpieczeństwa? | 149 |
| Czy firewall nie może służyć jako system IDS? | 150 |
| Jak jeszcze można poszukiwać śladów włamań?..... | 151 |
| Co jeszcze można zrobić za pomocą systemów wykrywania włamań? | 153 |
| Monitorowanie dostępu do baz danych..... | 153 |
| Monitorowanie funkcji serwerów DNS | 154 |
| Ochrona serwerów poczty elektronicznej | 154 |
| Wykorzystywanie systemu IDS do monitorowania przestrzegania polityki bezpieczeństwa firmy | 155 |
| Podsumowanie | 155 |

Część II Firewallle systemów Linux i Solaris..... 157

Rozdział 5. Firewallle iptables..... 159

| | |
|--|-----|
| Wprowadzenie | 159 |
| Potrzeba stosowania zapór sieciowych | 160 |
| Wybór komputera pełniącego rolę zapory sieciowej..... | 161 |
| Podstawy działania zapory iptables..... | 162 |
| Konfiguracja zapory iptables za pomocą tekstowej konsoli systemu Linux | 164 |
| Czyszczenie tablic i łańcuchów przetwarzania pakietów..... | 164 |
| Zerowanie liczników łańcuchów | 165 |
| Wyświetlanie listy reguł | 166 |
| Ustalanie domyślnej reguły przetwarzania pakietów | 167 |
| Tworzenie i niszczenie własnych łańcuchów przetwarzania pakietów | 168 |
| Modyfikowanie listy reguł przetwarzania pakietów | 168 |
| Opcje tworzące definicję reguły..... | 169 |
| Przykłady konfiguracji zapory iptables..... | 169 |
| Generalizowanie adresów IP i nazw interfejsów | 169 |
| Schemat filtrującej zapory sieciowej | 171 |
| Blokowanie wybranych adresów IP..... | 171 |
| Limitowanie ruchu ICMP..... | 172 |
| Udostępnianie połączenia internetowego..... | 173 |
| Przezroczyste pośrednictwo w połączeniu..... | 174 |
| Przekierowywanie portu do wnętrza sieci..... | 176 |
| Monitorowanie połączeń sieciowych..... | 176 |
| Zarządzanie zaporą iptables za pomocą graficznego interfejsu użytkownika | 177 |
| Podsumowanie | 181 |

Rozdział 6. Zarządzanie firewallami o otwartym kodzie źródłowym..... 183

| | |
|--|-----|
| Wprowadzenie | 183 |
| Testowanie firewalli..... | 184 |
| Fałszowanie adresów IP..... | 185 |
| Otwarte porty (uruchomione usługi)..... | 185 |
| Monitorowanie dysków twardych, pamięci RAM i pracy procesorów..... | 186 |
| Podejrzani użytkownicy, nietypowe dane uwierzytelniające i czas logowania..... | 186 |
| Weryfikacja bazy danych reguł..... | 187 |
| Sprawdzenie możliwości zestawiania połączeń..... | 187 |
| Skanowanie portów | 188 |
| Wykorzystanie aplikacji Telnet, Ipchains, Netcat i SendIP do badania firewalla | 189 |
| Ipchains..... | 189 |
| Telnet..... | 189 |

| | |
|---|------------|
| Netcat..... | 190 |
| SendIP — falszerek pakietów | 195 |
| Dzienniki pracy oraz opcje blokowania ruchu i generowania komunikatów | 198 |
| Firewall Log Daemon | 198 |
| Program fwlogwatch..... | 204 |
| Automatyzacja pracy programu fwlogwatch | 208 |
| Wykorzystanie aplikacji fwlogwatch i skryptów CGI | 215 |
| Dodatkowe narzędzia analizy zdarzeń firewala | 220 |
| Podsumowanie | 222 |
| Rozdział 7. System Solaris jako bezpieczny router i firewall | 223 |
| Wprowadzenie | 223 |
| System Solaris jako bezpieczny router..... | 224 |
| Uzasadnienie wyboru systemu Solaris..... | 224 |
| Warunki uruchomienia funkcji routingu..... | 225 |
| Konfiguracja routingu..... | 227 |
| Zwiększanie poziomu zabezpieczeń | 231 |
| Wymogi bezpieczeństwa | 231 |
| Wyłączenie funkcji routingu..... | 233 |
| Routing pakietów protokołu IP wersji 6..... | 235 |
| Pliki konfiguracyjne..... | 235 |
| Programy IPv6..... | 239 |
| Procedura uruchomienia routera IPv6..... | 241 |
| Wyłączenie funkcji routingu IPv6 | 242 |
| Stacje korzystające z protokołu IP w wersji 6..... | 244 |
| Automatyczna konfiguracja | 244 |
| Ręczna konfiguracja | 244 |
| System Solaris jako bezpieczna brama | 246 |
| System Solaris jako firewall..... | 246 |
| Teoria firewalli | 247 |
| Ogólny projekt firewala | 248 |
| SunScreen Lite..... | 249 |
| IP Filter | 250 |
| Wykorzystanie mechanizmu NAT | 250 |
| Podsumowanie | 251 |
| Część III Firewallle PIX..... | 253 |
| Rozdział 8. Wprowadzenie do firewalli PIX | 255 |
| Wstęp | 255 |
| Ogólna charakterystyka zapór PIX | 256 |
| Wbudowany system operacyjny | 256 |
| Algorytm ASA..... | 257 |
| Zaawansowana obsługa protokołów | 266 |
| Obsługa sieci VPN..... | 266 |
| Filtracja adresów URL..... | 267 |
| Translacja NAT i PAT | 268 |
| Ciągłość dostępu..... | 269 |
| Platformy sprzętowe PIX-a..... | 270 |
| Modele..... | 270 |
| Port konsoli..... | 274 |
| Licencje i uaktualnianie oprogramowania..... | 275 |
| Licencje | 276 |
| Uaktualnianie oprogramowania | 277 |
| Resetowanie haseł..... | 278 |

| | |
|--|------------|
| Korzystanie z wiersza poleceń | 280 |
| Konfiguracje domyślne | 280 |
| Tryby administracji | 281 |
| Podstawowe polecenia | 283 |
| Zarządzanie konfiguracjami | 287 |
| Restartowanie systemu | 289 |
| Podsumowanie | 290 |
| Rozdział 9. Kontrola ruchu sieciowego | 293 |
| Wprowadzenie | 293 |
| Obsługa ruchu wychodzącego | 293 |
| DYNAMICZNA translacja adresów | 294 |
| Blokowanie ruchu wychodzącego | 299 |
| Obsługa ruchu przychodzącego | 307 |
| Stacyczna translacja adresów | 308 |
| Listy dostępu | 309 |
| Ścieżki | 309 |
| Obsługa komunikatów ICMP | 310 |
| Przekierowywanie portów | 310 |
| Kompilowane listy dostępu — TurboACL | 312 |
| Grupowanie obiektów | 312 |
| Konfiguracja i wykorzystanie grup obiektów | 313 |
| Studium przypadku | 316 |
| Listy dostępu | 318 |
| Listy outbound i ścieżki | 320 |
| Podsumowanie | 322 |
| Rozdział 10. Zaawansowane funkcje firewalli PIX | 323 |
| Wprowadzenie | 323 |
| Obsługa protokołów o wyższym stopniu złożoności | 323 |
| FTP | 327 |
| DNS | 331 |
| SMTP | 333 |
| HTTP | 335 |
| Polecenia „r” | 335 |
| RPC | 336 |
| RTSP, NetShow i VDO Live | 338 |
| SQL*Net | 341 |
| Protokoły VoIP | 342 |
| SCCP | 344 |
| SIP | 345 |
| ILS i LDAP | 347 |
| Filtrowanie ruchu sieci WWW | 347 |
| Filtrowanie adresów URL | 348 |
| Filtrowanie wykonywalnej zawartości stron WWW | 353 |
| Obsługa DHCP | 355 |
| Firewall PIX jako klient DHCP | 356 |
| Firewall PIX jako serwer DHCP | 357 |
| Inne zaawansowane funkcje | 361 |
| Kontrola fragmentacji — FragGuard | 361 |
| AAA Floodguard | 363 |
| SYN Floodguard | 363 |
| Sprawdzanie trasy odwrotnej | 365 |
| Routing w trybie unicast | 367 |

| | |
|--|------------|
| Częściowy routing rozsyłania grupowego | 371 |
| PPPoE | 376 |
| Podsumowanie | 378 |
| Rozdział 11. Rozwiązywanie problemów i monitorowanie wydajności | 381 |
| Wprowadzenie | 381 |
| Rozwiązywanie problemów ze sprzętem i okablowaniem | 382 |
| Rozwiązywanie problemów ze sprzętem | 383 |
| Rozwiązywanie problemów z okablowaniem | 392 |
| Rozwiązywanie problemów z komunikacją | 395 |
| Weryfikacja adresowania | 396 |
| Weryfikacja trasowania | 397 |
| Weryfikacja translacji adresów | 402 |
| Weryfikacja dostępu | 405 |
| Rozwiązywanie problemów z IPsec | 409 |
| ISAKMP | 411 |
| IPsec | 414 |
| Przechwytywanie ruchu sieciowego | 417 |
| Wyświetlanie wyników przechwytywania | 418 |
| Przesyłanie wyników przechwytywania | 419 |
| Monitorowanie i rozwiązywanie problemów z wydajnością | 421 |
| Monitorowanie wydajności procesora | 422 |
| Monitorowanie stanu pamięci | 426 |
| Monitorowanie wydajności sieci | 428 |
| Wydajność firewalla PIX a protokół ident | 429 |
| Podsumowanie | 430 |
| | |
| Część IV Check Point NG i urządzenia Nokia IP Series | 433 |
| Rozdział 12. Instalowanie i konfigurowanie firewalla | |
| VPN-1/FireWall-1 Next Generation | 435 |
| Wprowadzenie | 435 |
| Zanim rozpoczniesz | 435 |
| Uzyskiwanie licencji | 437 |
| Zabezpieczanie komputera | 438 |
| Konfigurowanie interfejsów sieciowych | 440 |
| Konfigurowanie DNS | 442 |
| Przygotowanie do instalacji produktu VPN-1/FireWall-1 NG | 442 |
| Aktualizowanie wcześniejszej wersji | 447 |
| Instalowanie produktu Check Point VPN-1 /FireWall-1 NG w systemie Windows | 448 |
| Instalowanie z płyty CD | 449 |
| Konfigurowanie produktu Check Point VPN-1/FireWall-1 NG w systemie Windows | 458 |
| Usuwanie produktu Check Point VPN-1 /FireWall-1 NG w systemie Windows | 471 |
| Usuwanie produktu VPN-1 & FireWall-1 | 471 |
| Usuwanie pakietu SVN Foundation | 473 |
| Usuwanie klientów zarządzających | 474 |
| Instalowanie produktu Check Point VPN-1 /FireWall-1 NG w systemie Solaris | 475 |
| Instalowanie z płyty CD | 476 |
| Konfigurowanie produktu Check Point VPN-1/FireWall-1 NG w systemie Solaris | 481 |
| Usuwanie produktu Check Point VPN-1 /FireWall-1 NG w systemie Solaris | 493 |
| Usuwanie produktu VPN-1 & FireWall-1 | 493 |
| Usuwanie pakietu SVN Foundation | 496 |
| Usuwanie klientów zarządzających | 497 |

| | |
|--|------------|
| Instalowanie produktu Check Point VPN-1 /FireWall-1 NG na platformie Nokia | 498 |
| Instalowanie pakietu VPN-1/FireWall-1 NG | 499 |
| Konfigurowanie produktu VPN-1/FireWall-1 NG na platformie Nokia | 503 |
| Podsumowanie | 504 |
| Rozdział 13. Graficzny interfejs użytkownika | 507 |
| Wprowadzenie | 507 |
| Zarządzanie obiektami | 507 |
| Obiekty sieciowe | 509 |
| Usługi | 522 |
| Zasoby | 527 |
| Aplikacje OPSEC | 528 |
| Serwery | 528 |
| Użytkownicy wewnętrzni | 531 |
| Czas | 532 |
| Łącze wirtualne..... | 533 |
| Dodawanie reguł | 534 |
| Reguły..... | 534 |
| Właściwości globalne | 537 |
| Niejawne reguły FW-1..... | 537 |
| Panel Security Server..... | 539 |
| Panel Authentication..... | 539 |
| Panel VPN-1 | 539 |
| Panel Desktop Security..... | 540 |
| Panel Visual Policy Editor..... | 540 |
| Panel Gateway High Availability | 540 |
| Panel Management High Availability..... | 540 |
| Panel Stateful Inspection | 540 |
| Panel LDAP Account Management | 540 |
| Panel Network Address Translation | 540 |
| Panel ConnectControl | 540 |
| Panel Open Security Extension..... | 541 |
| Panel Log and Alert..... | 541 |
| Narzędzie SecureUpdate | 541 |
| Narzędzie Log Viewer | 543 |
| Wybór kolumn | 545 |
| Narzędzie System Status..... | 545 |
| Podsumowanie | 546 |
| Rozdział 14. Tworzenie zasad bezpieczeństwa | 549 |
| Wprowadzenie | 549 |
| Przyczyny tworzenia polityki bezpieczeństwa..... | 549 |
| Sposób tworzenia polityki bezpieczeństwa | 550 |
| Projekt zabezpieczeń..... | 552 |
| Architektura firewala | 553 |
| Tworzenie polityki..... | 553 |
| Wdrażanie polityki bezpieczeństwa | 557 |
| Zasady domyślne i wstępne | 557 |
| Przekształcanie polityki bezpieczeństwa do postaci reguł | 558 |
| Manipulowanie regułami | 569 |
| Opcje polityki | 571 |
| Instalowanie polityki bezpieczeństwa..... | 573 |
| Pliki polityki bezpieczeństwa..... | 574 |
| Podsumowanie | 575 |

| | |
|---|------------|
| Rozdział 15. Konfiguracje zaawansowane | 577 |
| Wprowadzenie | 577 |
| Moduł Check Point High Availability (CPHA) | 578 |
| Zapewnienie wysokiej dostępności | 578 |
| Przełączanie awaryjne | 580 |
| Synchronizacja firewalla | 581 |
| Konfiguracja z pojedynczym punktem wejściowym VPN | 583 |
| Konfigurowanie bramy | 584 |
| Konfigurowanie zasad polityki bezpieczeństwa | 588 |
| Konfiguracja z wieloma punktami wejściowymi VPN | 589 |
| Pokrywające domeny VPN | 590 |
| Konfigurowanie bramy | 592 |
| Pokrywanie domen VPN | 593 |
| Inne metody zapewniania wysokiej dostępności | 596 |
| Awaryjne przełączanie funkcji trasowania | 596 |
| Opcje sprzętowe | 597 |
| Podsumowanie | 598 |
| Rozdział 16. Konfigurowanie prywatnych sieci wirtualnych | 599 |
| Wprowadzenie | 599 |
| Schematy szyfrowania | 600 |
| Algorytmy szyfrowania; kryptografia symetryczna i asymetryczna | 600 |
| Metody wymiany kluczy — tunelowanie i szyfrowanie w miejscu | 602 |
| Funkcja skrótu i podpisy cyfrowe | 603 |
| Certyfikaty i ośrodki certyfikacji | 604 |
| Typy sieci VPN | 604 |
| Domeny VPN | 604 |
| Konfigurowanie sieci VPN z użyciem FWZ | 605 |
| Definiowanie obiektów | 605 |
| Dodawanie reguł VPN | 607 |
| Ograniczenia FWZ | 608 |
| Konfigurowanie sieci VPN z użyciem IKE | 609 |
| Definiowanie obiektów | 609 |
| Dodawanie reguł VPN | 610 |
| Testowanie sieci VPN | 613 |
| Uwagi dotyczące sieci zewnętrznych | 616 |
| Konfigurowanie sieci VPN z użyciem SecuRemote | 616 |
| Obiekt bramy lokalnej | 616 |
| Właściwości szyfrowania użytkownika | 617 |
| Reguły szyfrowania klienta | 619 |
| Instalowanie oprogramowania klienckiego SecuRemote | 620 |
| Użycie oprogramowania klienckiego SecuRemote | 622 |
| Dokonanie trwałych zmian w pliku objects_5_0.C | 623 |
| Funkcja Secure Domain Login | 624 |
| Podsumowanie | 625 |
| Rozdział 17. Przegląd platformy Nokia Security Platform | 627 |
| Wprowadzenie | 627 |
| Przedstawienie urządzeń Nokia IP Series | 628 |
| Modele korporacyjne | 628 |
| Proste administrowanie systemem | 635 |
| Podsumowanie | 638 |

| | |
|--|------------|
| Rozdział 18. Konfigurowanie firewalla Check Point..... | 639 |
| Wprowadzenie | 639 |
| Przygotowanie do konfiguracji | 639 |
| Uzyskiwanie licencji..... | 640 |
| Konfigurowanie nazwy komputera..... | 641 |
| Opcje produktu FireWall-1 | 641 |
| Konfigurowanie firewalla | 643 |
| Instalowanie pakietów | 644 |
| Włączanie pakietów | 645 |
| Przekazywanie IP i polityki firewalla | 647 |
| Uruchomienie narzędzia cpconfig | 650 |
| Testowanie konfiguracji..... | 659 |
| Testowanie dostępu klientów GUI..... | 660 |
| Przesyłanie i pobieranie polityki..... | 663 |
| Aktualizowanie firewalla | 667 |
| Aktualizowanie z wersji 4.1 SP6 do wersji NG FP2..... | 668 |
| Aktualizowanie z wersji NG FP2 do wersji NG FP3 | 670 |
| Cofnięcie aktualizacji produktu 4.1 do wersji NG | 671 |
| Podsumowanie | 671 |
| Rozdział 19. Przedstawienie interfejsu Voyager | 673 |
| Wprowadzenie | 673 |
| Podstawowa konfiguracja systemu | 673 |
| Ekran początkowy..... | 674 |
| Konfigurowanie podstawowych danych interfejsu sieciowego | 676 |
| Dodawanie bramy domyślnej | 682 |
| Konfigurowanie czasu, daty i strefy czasowej | 684 |
| Konfigurowanie DNS i wpisów komputerów | 687 |
| Konfigurowanie przekazywania poczty | 690 |
| Konfigurowanie powiadomień o zdarzeniach systemowych | 691 |
| Konfigurowanie systemu w zakresie bezpieczeństwa..... | 691 |
| Włączanie dostępu poprzez SSH | 692 |
| Wyłączenie dostępu poprzez Telnet..... | 695 |
| Alternatywa dla protokołu FTP | 695 |
| Zabezpieczanie protokołu FTP | 696 |
| Konfigurowanie protokołu SSL..... | 698 |
| Opcje konfiguracyjne..... | 701 |
| Interface Configuration..... | 701 |
| System Configuration | 702 |
| SNMP | 703 |
| IPv6 | 703 |
| Reboot, Shut Down System | 703 |
| Security and Access Configuration..... | 703 |
| Fault Management Configuration | 704 |
| Routing Configuration | 704 |
| Traffic Management | 705 |
| Router Services..... | 706 |
| Podsumowanie | 707 |
| Rozdział 20. Administrowanie systemem w zakresie podstawowym..... | 709 |
| Wprowadzenie | 709 |
| Restartowanie systemu..... | 709 |
| Zarządzanie pakietami | 711 |
| Instalowanie pakietów | 711 |
| Włączanie i wyłączanie pakietów | 715 |
| Usuwanie pakietów..... | 717 |

| | |
|--|-----|
| Zarządzanie obrazami IPSO..... | 717 |
| Aktualizacja do nowszej wersji obrazu IPSO | 718 |
| Usuwanie obrazów IPSO | 721 |
| Zarządzanie użytkownikami i grupami | 721 |
| Użytkownicy..... | 722 |
| Grupy | 725 |
| Konfigurowanie tras statycznych..... | 727 |
| Archiwizacja i odtwarzanie systemu | 728 |
| Zestawy konfiguracji | 729 |
| Tworzenie kopii zapasowej..... | 730 |
| Odtwarzanie z kopii zapasowej..... | 733 |
| Protokołowanie | 734 |
| Protokołowanie lokalne | 734 |
| Protokołowanie zdalne..... | 735 |
| Dzienniki kontroli..... | 736 |
| Planowanie zadań cron | 736 |
| Podsumowanie | 738 |

Rozdział 21. Wysoka dostępność i klastry741

| | |
|--|-----|
| Wprowadzenie | 741 |
| Projektowanie klastra..... | 741 |
| Dlaczego klastry?..... | 741 |
| Wysoka dostępność czy podział obciążenia?..... | 742 |
| Obsługa klastrów w produktach Check Point | 743 |
| Łączenie klastra z siecią — przełączniki czy koncentratory? | 746 |
| Funkcje FireWall-1, pojedyncze bramy i klastry — podobieństwa i różnice..... | 747 |
| Instalowanie produktu FireWall-1 NG FP3 | 749 |
| Sprawdzenie wymagań wstępnych instalacji | 749 |
| Opcje instalacji | 750 |
| Procedura instalacji..... | 750 |
| Check Point ClusterXL | 754 |
| Konfigurowanie produktu ClusterXL w trybie HA New mode | 754 |
| Testowanie produktu ClusterXL w trybie HA New mode | 770 |
| Sposób działania produktu ClusterXL w trybie HA New mode | 774 |
| Specjalne uwagi dla produktu ClusterXL w trybie HA New mode | 780 |
| Konfigurowanie produktu ClusterXL w trybie HA Legacy mode | 783 |
| Konfigurowanie produktu ClusterXL w trybie podziału obciążenia..... | 784 |
| Testowanie produktu ClusterXL w trybie podziału obciążenia | 785 |
| Sposób działania produktu ClusterXL w trybie podziału obciążenia..... | 789 |
| Specjalne uwagi dla produktu ClusterXL w trybie podziału obciążenia..... | 792 |
| Klastry w systemie Nokia IPSO..... | 793 |
| Konfigurowanie klastra Nokia | 793 |
| Konfiguracja produktu Check Point FireWall-1 dla klastra Nokia | 795 |
| Konfigurowanie klastra Nokia w interfejsie Voyager..... | 800 |
| Testowanie klastra Nokia..... | 804 |
| Sposób działania klastrów Nokia | 810 |
| Specjalne uwagi dla klastrów Nokia | 814 |
| Klastry VRRP w systemie Nokia IPSO | 815 |
| Konfigurowanie klastra Nokia VRRP..... | 815 |
| Konfigurowanie klastra Nokia VRRP w interfejsie Voyager | 817 |
| Testowanie klastra Nokia VRRP | 822 |
| Sposób działania klastrów VRRP | 824 |
| Specjalne uwagi dla klastrów Nokia VRRP..... | 827 |
| Rozwiązania klastrowe innych firm..... | 827 |

| | |
|--|-----|
| Klasy i strojenie wydajności funkcji wysokiej dostępności..... | 828 |
| Przepustowość danych i duża liczba połączeń..... | 828 |
| Podsumowanie..... | 836 |

Część V Serwer ISA839

Rozdział 22. Planowanie i projektowanie wdrożenia serwera ISA.....841

| | |
|---|-----|
| Wprowadzenie..... | 841 |
| Wdrożenie serwera ISA — zagadnienia dotyczące planowania i projektowania..... | 841 |
| Szacowanie wymagań sieciowych i sprzętowych..... | 842 |
| Wymagania systemowe..... | 842 |
| Wymagania programowe..... | 843 |
| Wymagania sprzętowe..... | 843 |
| Zastosowanie usługi Active Directory..... | 853 |
| Zagadnienia o krytycznym znaczeniu..... | 854 |
| Odporność na uszkodzenia dysków twardej..... | 854 |
| Planowanie właściwego trybu instalacji..... | 863 |
| Instalacja w trybie firewalla..... | 864 |
| Instalacja w trybie bufora..... | 864 |
| Instalacja w trybie zintegrowanym..... | 865 |
| Konfiguracja samodzielna a macierzowa..... | 865 |
| Planowanie konfiguracji klientów ISA..... | 866 |
| Łączność z internetem oraz zagadnienia związane z systemem DNS..... | 871 |
| Podsumowanie..... | 874 |

Rozdział 23. Instalacja programu ISA Server.....875

| | |
|--|-----|
| Wprowadzenie..... | 875 |
| Organizacja planu instalacji..... | 875 |
| Pliki instalacyjne i uprawnienia..... | 876 |
| Klucz produktu oraz licencja produktu..... | 876 |
| Uwagi dotyczące Active Directory..... | 877 |
| Tryb serwera..... | 877 |
| Lokalizacja plików programu ISA Server na dysku..... | 877 |
| Identyfikatory występujące w sieci wewnętrznej a tabela adresów lokalnych..... | 878 |
| Instalacja dodatkowych funkcji programu ISA Server..... | 878 |
| Przebieg instalacji..... | 879 |
| Instalacja programu ISA Server — krok po kroku..... | 879 |
| Rozszerzenie serwera samodzielnego do elementu macierzy — krok po kroku..... | 889 |
| Zmiany wprowadzone na skutek instalacji programu ISA Server..... | 897 |
| Migracja z programu Microsoft Proxy Server 2.0..... | 898 |
| Co podlega przeniesieniu, a co nie?..... | 898 |
| Uaktualnienie programu Proxy Server 2.0 na platformie Windows 2000..... | 903 |
| Uaktualnienie programu Proxy Server 2.0 na platformie Windows NT..... | 906 |
| Podsumowanie..... | 908 |

Rozdział 24. Administrowanie serwerem ISA.....911

| | |
|---|-----|
| Wprowadzenie..... | 911 |
| Koncepcja administracji zintegrowanej..... | 911 |
| Konsola ISA Management..... | 912 |
| Kreatory ISA..... | 935 |
| Wykonywanie typowych zadań administracyjnych..... | 936 |
| Konfiguracja uprawnień do obiektów..... | 937 |
| Administrowanie macierzą..... | 939 |

| | |
|---|-------------|
| Korzystanie z funkcji monitorowania, alarmowania, rejestracji oraz raportowania..... | 941 |
| Tworzenie, konfiguracja i monitorowanie alarmów | 941 |
| Sesje monitorowania..... | 946 |
| Korzystanie z rejestracji..... | 948 |
| Generowanie raportów..... | 953 |
| Koncepcja administracji zdalnej | 964 |
| Instalacja konsoli ISA Management | 964 |
| Zdalne administrowanie serwerem ISA z wykorzystaniem usług Terminal Services.. | 966 |
| Podsumowanie | 971 |
| Rozdział 25. Optymalizacja, dostosowywanie, integracja | |
| oraz tworzenie kopii bezpieczeństwa serwera ISA | 973 |
| Wprowadzenie | 973 |
| Optymalizacja wydajności serwera ISA..... | 973 |
| Ustalanie linii odniesienia i monitorowanie wydajności..... | 975 |
| Postępowanie z typowymi problemami z wydajnością..... | 997 |
| Dostosowywanie programu ISA Server do własnych potrzeb | 1008 |
| Korzystanie z pakietu ISA Server SDK | 1009 |
| Korzystanie z dodatków niezależnych firm | 1012 |
| Integracja programu ISA Server z innymi usługami | 1014 |
| Współpraca z Active Directory..... | 1014 |
| Współpraca z usługami Routing and Remote Access | 1016 |
| Współpraca z usługą IIS | 1017 |
| Współpraca z protokołem IPSecurity..... | 1018 |
| Integracja programu ISA Server z domeną Windows NT 4.0..... | 1021 |
| Tworzenie kopii zapasowych i przywracanie konfiguracji serwera ISA..... | 1021 |
| Zasady tworzenia kopii zapasowych..... | 1022 |
| Tworzenie kopii zapasowej i przywracanie konfiguracji serwerów samodzielnych..... | 1022 |
| Tworzenie kopii zapasowej i przywracanie konfiguracji macierzy i przedsiębiorstwa | 1024 |
| Podsumowanie | 1026 |
| Rozdział 26. Rozwiązywanie problemów z serwerem ISA..... | 1027 |
| Wprowadzenie | 1027 |
| Wskazówki dotyczące rozwiązywania problemów | 1027 |
| Pięć kroków rozwiązywania problemu | 1028 |
| Rozwiązywanie problemów z instalacją i konfiguracją programu ISA Server | 1040 |
| Problemy ze zgodnością sprzętową i programową | 1040 |
| Problemy związane z konfiguracją początkową | 1041 |
| Rozwiązywanie problemów z uwierzytelnianiem i dostępem..... | 1044 |
| Problemy z uwierzytelnianiem..... | 1044 |
| Problemy z dostępem..... | 1047 |
| Problemy z połączeniami komutowanymi i połączeniami typu VPN..... | 1049 |
| Rozwiązywanie problemów klientów serwera ISA..... | 1051 |
| Problemy wydajnościowe klientów | 1051 |
| Problemy klientów z połączeniami | 1052 |
| Rozwiązywanie problemów z buforowaniem i udostępnianiem | 1055 |
| Problemy z buforowaniem | 1055 |
| Problemy z udostępnianiem..... | 1056 |
| Podsumowanie | 1058 |
| Rozdział 27. Zaawansowane udostępnianie serwerów przy użyciu serwera ISA... 1061 | |
| Wprowadzenie | 1061 |
| Wyłączanie mechanizmu puli gniazd..... | 1065 |
| Wyłączanie puli gniazd usług WWW oraz FTP | 1066 |
| Wyłączanie puli gniazd usług SMTP oraz NNTP..... | 1068 |
| Wyłączanie usług IIS na serwerze ISA..... | 1069 |

| | |
|---|-------------|
| Udostępnianie serwera | 1070 |
| Udostępnianie usług terminalowych działających w sieci wewnętrznej | 1070 |
| Udostępnianie usług terminalowych na serwerze ISA | 1075 |
| Jednoczesne udostępnianie usług terminalowych na serwerze ISA oraz w sieci wewnętrznej | 1078 |
| Udostępnianie witryn TSAC | 1079 |
| Udostępnianie serwerów FTP znajdujących się w sieci wewnętrznej | 1089 |
| Udostępnianie serwerów FTP umieszczonych na serwerze ISA | 1100 |
| Zastosowanie reguł udostępniania treści WWW w celu umożliwienia bezpiecznego dostępu FTP | 1108 |
| Udostępnianie serwerów HTTP oraz HTTPS (SSL) przy użyciu reguł udostępniania serwerów | 1113 |
| Udostępnianie hosta pcAnywhere umieszczonego w sieci wewnętrznej | 1117 |
| Publikacja treści WWW | 1120 |
| Moduły nasłuchujące Incoming Web Requests | 1121 |
| Zestawy miejsc docelowych | 1122 |
| Wpisy w publicznym systemie DNS | 1123 |
| Wpisy w prywatnym systemie DNS | 1123 |
| Zakończenie połączenia SSL na serwerze ISA | 1125 |
| Mostkowanie połączeń SSL | 1142 |
| Bezpieczne połączenia FTP wykorzystujące protokół SSL | 1151 |
| Udostępnianie serwera certyfikatów | 1153 |
| Podsumowanie | 1156 |
| Rozdział 28. Ochrona usług pocztowych przy użyciu serwera ISA | 1157 |
| Wprowadzenie | 1157 |
| Konfiguracja usług pocztowych na serwerze ISA | 1158 |
| Udostępnianie usługi IIS SMTP na serwerze ISA | 1159 |
| Program Message Screener na serwerze ISA | 1166 |
| Udostępnianie serwera Exchange na serwerze ISA | 1170 |
| Udostępnianie usługi Outlook Web Access na serwerze ISA | 1197 |
| Program Message Screener na serwerze ISA oraz Exchange | 1207 |
| Konfiguracja usług pocztowych w sieci wewnętrznej | 1213 |
| Udostępnianie serwera Exchange umieszczonego w sieci wewnętrznej | 1214 |
| Udostępnianie usługi RPC serwera Exchange | 1216 |
| Udostępnianie witryny Outlook Web Access uruchomionej na wewnętrznym serwerze Exchange | 1223 |
| Program Message Screener na wewnętrznym serwerze Exchange | 1225 |
| Oprogramowanie MailSecurity oraz MailEssentials firmy GFI przeznaczone dla serwerów SMTP | 1228 |
| Wersje programu MailSecurity | 1230 |
| Instalacja programu MailSecurity dla bram SMTP | 1230 |
| Konfiguracja programu MailSecurity | 1233 |
| Podsumowanie | 1239 |
| Część VI Wykrywanie włamań | 1241 |
| Rozdział 29. Snort — wprowadzenie | 1243 |
| Wprowadzenie | 1243 |
| Do czego służy aplikacja Snort? | 1244 |
| Wymagania systemowe aplikacji Snort | 1246 |
| Wymagania sprzętowe | 1246 |
| Funkcje aplikacji Snort | 1248 |
| Monitor pakietów | 1249 |
| Preprocesor | 1249 |

| | |
|---|-------------|
| Mechanizm detekcji włamań | 1250 |
| Moduł rejestracji danych i generowania komunikatów alarmowych | 1251 |
| Wykorzystanie aplikacji Snort w sieci | 1252 |
| Zastosowanie aplikacji Snort | 1254 |
| Program Snort a architektura sieci | 1259 |
| Wady programu Snort | 1262 |
| Bezpieczeństwo aplikacji Snort | 1264 |
| Snort jest aplikacją podatną na ataki | 1264 |
| Zabezpieczanie systemu Snort | 1265 |
| Podsumowanie | 1266 |
| Rozdział 30. Instalacja programu Snort | 1267 |
| Wprowadzenie | 1267 |
| Krótki opis dystrybucji systemu Linux | 1268 |
| Debian | 1268 |
| Slackware | 1268 |
| Gentoo | 1269 |
| Instalacja biblioteki PCAP | 1270 |
| Instalacja biblioteki libcap z plików źródłowych | 1271 |
| Instalacja biblioteki libcap z pakietu RPM | 1274 |
| Instalacja programu Snort | 1275 |
| Instalacja programu Snort z plików źródłowych | 1275 |
| Konfigurowanie aplikacji Snort — edycja pliku snort.conf | 1276 |
| Instalacja pakietu RPM programu Snort | 1279 |
| Instalacja programu Snort w systemie Windows | 1281 |
| Instalacja najnowszych wersji programu Snort | 1284 |
| Podsumowanie | 1284 |
| Rozdział 31. Łączenie firewalli i systemów IDS | 1287 |
| Wprowadzenie | 1287 |
| Systemy IDS o określonej polityce działania | 1287 |
| Definiowanie polityki działania systemów IDS | 1289 |
| Przykład konfiguracji systemu | 1293 |
| Wdrażanie systemów IDS o określonej polityce działania | 1297 |
| Aktywne systemy IDS | 1300 |
| Powstanie aktywnego systemu IDS w projekcie Snort | 1301 |
| Instalacja programu Snort w trybie aktywnym | 1301 |
| Wykorzystanie aktywnego systemu IDS do ochrony sieci | 1313 |
| Funkcje IDS w firewallu PIX | 1316 |
| Sygnatury | 1316 |
| Konfigurowanie pracy firewalli PIX z systemami IDS | 1319 |
| Konfiguracja wykluczeń | 1322 |
| Podsumowanie | 1323 |
| Dodatki | 1325 |
| Skorowidz | 1327 |

Rozdział 11.

Rozwiązywanie problemów i monitorowanie wydajności

Wprowadzenie

Ten rozdział poświęcony jest rozwiązywaniu problemów z firewallami PIX. Po opanowaniu składni poleceń i podstawowych funkcji firewalla, PIX jawi się jako urządzenie względnie proste do skonfigurowania. Zbiór poleceń PIX-a jest mały w porównaniu do zbioru poleceń dostępnych na routerach i przełącznikach firmy Cisco. W poprzednich rozdziałach firewall PIX został omówiony dość szczegółowo, począwszy od różnic w platformach sprzętowych, poprzez konfigurację podstawową do zaawansowanej. Książka ta zawiera informacje o sposobach integracji firewalli PIX z już istniejącymi sieciami. Bez względu na to, jak dobrze skonfigurowano PIX-a, problemy mogą pojawić się zawsze — ich rozwiązanie leży w gestii administratora. Celem niniejszego rozdziału jest przedstawienie metod, które pozwalają na skuteczne rozwiązywanie różnych problemów i dostarczenie wiedzy o najważniejszych krokach, jakie należy podjąć w przypadku sytuacji krytycznej.

Problemy ze sprzętem i okablowaniem mogą stanowić zmurę sieci, w której wszystko ponadto jest zupełnie w porządku. Źródło problemów ze sprzętem często staje się oczywiste po spojrzeniu na odpowiednie diody kontrolne. Rozwiązywanie problemów znacznie ułatwia fakt, iż liczba standardów okablowania, jakie obsługuje PIX, jest niewielka. W rozdziale tym zawarte są również techniczne informacje na temat okablowania, rozdział ten może być cenną pomocą podczas weryfikacji jego poprawności.

Firewall PIX stanowi urządzenie przetwarzające ruch IP. Choć jest to urządzenie bardzo wyspecjalizowane, które realizuje wiele funkcji związanych z bezpieczeństwem, to jednak pozostaje tylko i wyłącznie urządzeniem, które obsługuje ruch IP. Jako takie musi wiedzieć, jak trasować tego typu ruch. W rozdziale zwrócono uwagę na kilka powszechnych problemów z komunikacją, przedstawiono również odpowiednie sposoby ich rozwiązywania. Wartościową funkcją PIX-a jest obsługa translacji adresów, która pozwala na oszczędne gospodarowanie dostępną przestrzenią publicznych adresów IP oraz ukrywanie informacji o wewnętrznej strukturze chronionej sieci. I tu — w przypadku jakichkolwiek problemów — administrator musi dysponować odpowiednimi metodami, które pozwolą na odszukanie źródła problemów i rozwiązanie ich.

Zapora PIX daje możliwość wykorzystania kilku różnych mechanizmów kontroli dostępu — od prostych list dostępu do złożonych kombinacji ścieżek. Mechanizmy kontroli dostępu nacechowane są różnymi mniej i bardziej precyzyjnymi informacjami, określającymi sposób kontroli ruchu. Rozwiązywanie problemów z kontrolą dostępu to nie tylko rozwiązywanie problemów z możliwością dostępu do określonych zasobów, to również odnajdywanie pewnej równowagi, w której odpowiedni ruch jest przepuszczany, a odpowiedni jest blokowany.

O IPsec powstały całe książki, i to nie bez przyczyny. IPsec pozwala na ochronę ruchu, która realizowana jest bezpośrednio przez dwa komunikujące się ze sobą hosty — nie istnieje tu konieczność specjalnej obsługi komunikacji na poszczególnych węzłach ścieżki. Konfiguracja IPsec może być bardzo złożona. Realizacja obsługi, a tym bardziej rozwiązywanie problemów z IPsec, wymaga dobrej znajomości tematu. W rozdziale tym przedstawiono tylko kilka zasadniczych kwestii związanych z IPsec, głównie z IKE (ang. *IPsec Key Exchange*, wymiana kluczy IPsec), mamy nadzieję — przydatnych.

Często podczas rozwiązywania problemów skuteczną pomocą okazuje się możliwość przechwytywania pakietów. Analiza przechwyconego ruchu często ułatwia identyfikację źródła problemów. W zakresie przechwytywania ruchu firewall PIX daje możliwość wykorzystania kilku różnych funkcji, dostępnych poprzez odpowiednie polecenia. Do dekodowania i analizy pakietów można posłużyć się narzędziami innych firm — niektóre z nich zostały tu przedstawione.

W jaki sposób stwierdzić, czy firewall PIX pracuje tak wydajnie, jak powinien? Jak stwierdzić, czy jest przeciążony? Wydajność firewalla i jego stan powinny być monitorowane w sposób aktywny. Celem takiego działania jest uniknięcie sytuacji, w której drobne problemy obracają się w wielkie. Wyniki procesu monitorowania mogą być całkiem obszerne i trudne do interpretacji, do wyciągnięcia wniosków jest tu konieczna dobra znajomość rzeczy.

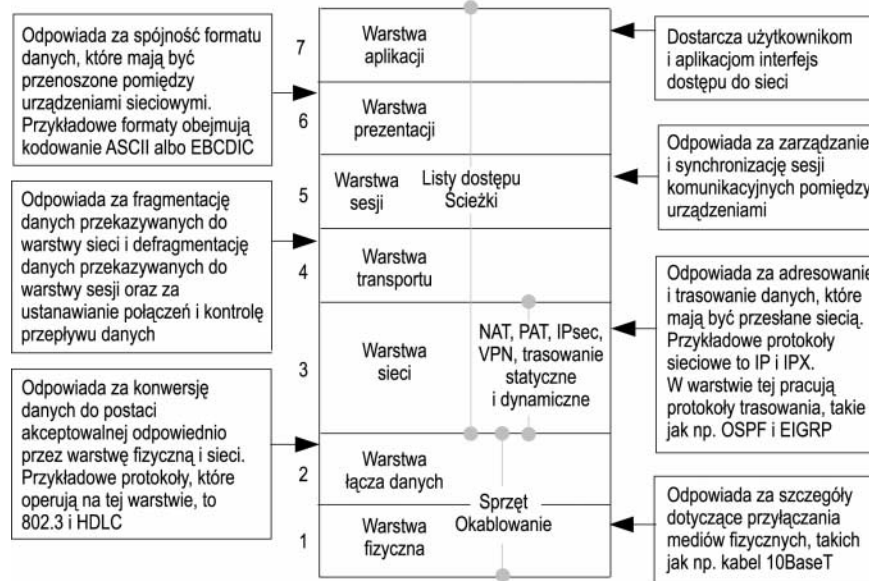
Rozwiązywanie problemów ze sprzętem i okablowaniem

Najważniejszą rzeczą, związaną z rozwiązywaniem wszelkich problemów, jest traktowanie ich w sposób logiczny i metodyczny — dzięki temu żaden ważny krok nie zostanie pominięty. Struktura i funkcje sieci mają naturę modułową. Często konieczne jest sprawdzenie poprawności funkcjonowania wszystkich komponentów firewalla.

Dobłą pomocą podczas rozwiązywania problemów z firewallem PIX jest tzw. model OSI. Model ten powstał jako model referencyjny, służący jako punkt odniesienia podczas tworzenia rozwiązań sieciowych. Główną jego cechą jest podział funkcji na warstwy. Rozważając komunikujące się ze sobą hosty, zauważymy, że komunikacja ta zachodzi pomiędzy równorzędnymi warstwami na obu hostach — np. warstwa sieci na jednym hoście komunikuje się z warstwą sieci na drugim hoście.

Proponowane w tym rozdziale podejście opiera metodę rozwiązywania problemów właśnie na modelu OSI, jest on przedstawiony na rysunku 11.1. Problemy rozpatrywane są począwszy od warstwy najniższej, tj. warstwy fizycznej — tu będą istotne np. sprawdzenie

Rysunek 11.1.
Model OSI



działania sprzętu i okablowania. Dopiero po zweryfikowaniu poprawności działania komponentów danej warstwy można zacząć zajmować się komponentami właściwymi warstwie wyższej.

Przedstawione w rozdziale sposoby radzenia sobie z problemami uporządkowane są zgodnie z warstwami modelu OSI. Rozwiązywanie problemów należy rozpocząć od warstwy fizycznej. Po sprawdzeniu poprawności działania wszystkich komponentów fizycznych uwaga powinna zostać zwrócona ku komponentom warstwy łączy danych i tak dalej — w górę warstw modelu OSI. Obranie takiej metody gwarantuje, że żaden aspekt istniejącej konfiguracji nie zostanie pominięty — nie zostanie zatem pominięte żadne źródło błędów¹.

Nasze rozważania rozpoczniemy od krótkiej prezentacji architektury sprzętowej i okablowania PIX-a.

Rozwiązywanie problemów ze sprzętem

Podczas sprawdzania konfiguracji i rozwiązywania problemów pomocna może być znajomość technicznych szczegółów każdego z modeli PIX-a. Wiedza ta może przyspieszyć proces rozwiązywania problemów już od samego początku, gdyż pozwala na określenie sposobu interpretacji postrzegalnych symptomów. Jeżeli do realizacji założonych celów wykorzystywany jest niewłaściwy model firewala, to pracy jego nie da się usprawnić w żaden z przedstawionych w rozdziale sposobów.

¹ W związku z takim, a nie innym rozdzieleniem funkcji w modelu OSI — w obranej metodzie bardziej istotne jest raczej to, iż polega ona na eliminowaniu źródeł błędów w kolejności: od funkcji podstawowych do funkcji na nich opartych. To, że żadne źródło błędów nie zostanie pominięte, jest tylko naturalną konsekwencją, istotna jest optymalność całego procesu — *przyp. thum*.

Można powiedzieć, iż rozwiązywanie problemów zaczyna się już w momencie planowania sieci i polityki bezpieczeństwa. Istnieje kilka rodzajów firewalle PIX, każdy z nich jest zdolny do obsługi różnej liczby różnych rodzajów interfejsów sieciowych. Każdy z modeli ma określoną górną granicę liczby równocześnie obsługiwanych połączeń — wartości te zebrano w tabeli 11.1, prezentuje ona tylko wycinek informacji charakteryzujących poszczególne modele.

Tabela 11.1. Wybrane parametry firewalle PIX

| Model | Obsługiwane rodzaje interfejsów | Maksymalna liczba interfejsów | Obsługa ciągłości dostępu |
|----------|---------------------------------|---|---------------------------|
| PIX 501 | Ethernet | Jeden port 10 Mb/s umieszczony na stałe. | Nie |
| | Fast Ethernet 10BaseT | Czteroportowy przełącznik 10/100 Mb/s wbudowany na stałe. | |
| PIX 506E | Ethernet | Dwa porty 10/100 Mb/s umieszczone na stałe. | Nie |
| | Fast Ethernet | | |
| PIX 515E | Ethernet | Dwa porty 10/100 Mb/s umieszczone na stałe. | Tak |
| | Fast Ethernet | Dwa gniazda interfejsów. Maksymalnie 6 portów. | |
| PIX 525 | Ethernet | Dwa porty 10/100 Mb/s umieszczone na stałe. | Tak |
| | Fast Ethernet | Cztery gniazda interfejsów. | |
| | Gigabit Ethernet | Maksymalnie 8 portów. | |
| PIX 535 | Ethernet | Dziewięć gniazd interfejsów. | Tak |
| | Fast Ethernet | Maksymalnie 10 portów. | |
| | Gigabit Ethernet | | |

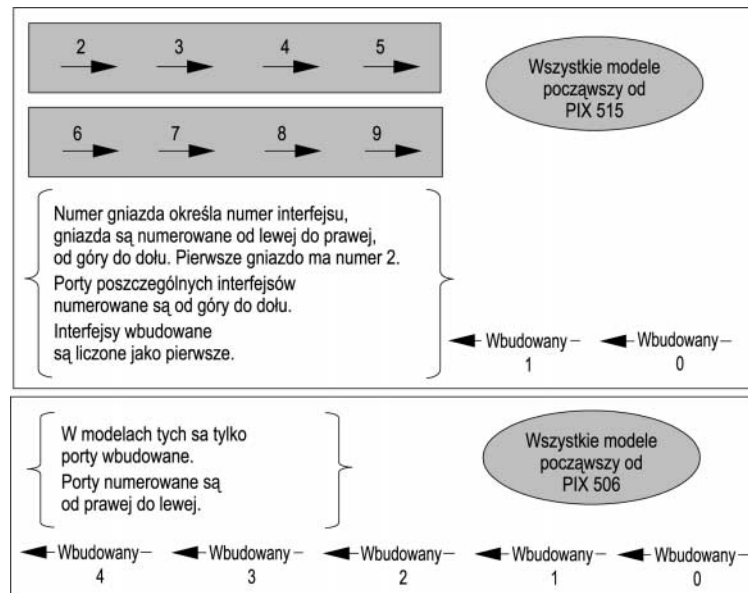
Moduł FWSM 1.1 (ang. *Firewall Services Module*) przeznaczony dla przełączników z serii Catalyst 6500 nie ma żadnych fizycznych interfejsów. Zamiast tego daje możliwość podłączenia do 100 interfejsów VLAN. Obsługa ciągłości dostępu realizowana jest poprzez wydzielony do tego celu interfejs logiczny.

Wiedza o tym, czy wykorzystywany model firewalle PIX jest adekwatny do potrzeb — jest ważna. Na przykład mając sieć, w której firewall będzie musiał realizować 100000 równoczesnych połączeń, a firewallem tym ma być PIX 501, to będzie on przeciążony, a to z kolei doprowadzi do niestabilności. W scenariuszu tym żadne rozwiązywanie problemów ani konfigurowanie zapory nie sprawi, że firewall ten sprosta wyzwaniu — po prostu nie jest on przeznaczony do obsługi ruchu o takim natężeniu. O możliwościach obsługi ruchu o danym natężeniu decyduje wydajność danego modelu, to ona jest tu istotna. Przeciążenie firewalle prowadzi do awarii albo powstawania zatorów. Niedociążenie firewalle, choć bardzo korzystne z wydajnościowego punktu widzenia, może jednak stanowić stratę z punktu widzenia niewykorzystanych mocy czy stopnia zwrotu inwestycji. Na przykład jeśli w danej sieci nigdy nie będzie więcej aniżeli 200 równoczesnych połączeń, to instalowanie PIX-a 535 oznaczać będzie stratę — inwestycja w sprzęt i oprogramowanie pozostanie niewykorzystana, wydajność jednakże będzie rewelacyjna.

Jak przedstawiono w tabeli 11.1 — różne modele dają możliwość wykorzystania różnych rodzajów interfejsów w określonej liczbie. W tabeli tej nie został uwzględniony fakt, iż kilka modeli obsługuje również interfejsy Token Ring i FDDI. Począwszy od wprowadzenia oprogramowania PIX-a w wersji 5.3, firma Cisco przerwała obsługę sieci Token Ring i FDDI. Różne inne od Ethernetu interfejsy obsługiwane są począwszy od modelu PIX 515. Jako regułę można przyjąć zalecenie, by na jednej zaporze nie wykorzystywać interfejsów różnych rodzajów — PIX powinien być skonfigurowany do obsługi tylko jednego rodzaju sieci. Tak więc na danym firewallu wszystkie interfejsy powinny być interfejsami Ethernet albo interfejsami Token Ring, albo wszystkie powinny być interfejsami FDDI. Utrzymanie tego rodzaju „czystości” sieci redukuje obciążenie zapory — PIX nie musi dokonywać konwersji pomiędzy różnymi formatami ramek.

Firewall PIX posiada określony sposób numerowania interfejsów sieciowych, bez zrozumienia go — rozwiązywanie problemów mija się z celem. Bez znajomości sposobu, w jaki są numerowane i identyfikowane interfejsy, marnuje się cenny czas, który mógłby być poświęcony właściwemu rozwiązywaniu problemów. Sposób numeracji interfejsów przedstawia rysunek 11.2. Numeracja kart interfejsów zaczyna się od prawej strony, pierwszy jest interfejs 0, numery rosną do lewej. Numer gniazda, w którym jest instalowana karta, określa numer przypisywany tej karcie. Porty karty numerowane są od góry do dołu, zaczynając od 0 dla portu znajdującego się w górnej części karty.

Rysunek 11.2.
Numeracja
interfejsów
firewalli PIX



Na przykład najwyżej położony port na karcie umieszczonej w trzecim gnieździe będzie identyfikowany jako Ethernet 3/0. Interfejsy umieszczone na stałe zaczynają się od numeru 0 z prawej strony, kolejny w lewo będzie rozpoznawany jako 1. Pierwsza zainstalowana karta interfejsów będzie oznaczona numerem 2 (umieszczona jest właśnie w drugim gnieździe), a jej pierwszy interfejs od góry — 0. Przyswojenie przedstawionego schematu identyfikowania kart i interfejsów daje pewność, że konfiguracja czy też wysiłki mające na celu rozwiązanie jakichś problemów — koncentrują się na właściwym interfejsie.

Architektura pamięci firewalli PIX jest w pewien sposób podobna do tej znanej z routerów Cisco, wyjątkiem jest brak pamięci NVRAM. Pamięć flash jest w PIX-ie wykorzystywana do przechowywania systemu operacyjnego firewalla (tj. jego obrazu) i przechowywania pliku konfiguracji. Pamięć RAM jest wykorzystywana do przetwarzania danych. Regułą jest, że rozmiar pamięci flash powinien umożliwiać przechowywanie obrazu systemu operacyjnego i całej konfiguracji firewalla. Rozważając wszystkie rodzaje pamięci, pamięć RAM determinuje wydajność w stopniu najwyższym — jest ona przestrzenią roboczą firewalla. Wszelkie dane, które oczekują na przetworzenie albo też mają zostać przekazane do któregoś z interfejsów, przechowywane są właśnie w pamięci RAM. Zalecane jest, by rozmiar pamięci RAM był jak największy. Gdy pamięci RAM jest za mało — następuje wzrost liczby utraconych pakietów, a ruch jest przekazywany wolniej.

Każdy PIX ma kilka diod LED, które dają wizualne sygnały, informujące o stanie firewalla. W przypadku różnych modeli liczba i znaczenie diod są inne, jednakże część z nich we wszystkich modelach PIX-a ma to samo znaczenie — ich opis przedstawiono na rysunku 11.3. Zapoznanie się z ich znaczeniem pozwoli na rozpoczęcie rozwiązywania problemów, leżących w warstwie fizycznej, od zewnętrznych „ogłędzin” firewalla.

Rysunek 11.3.
Wybrane wskaźniki
LED firewalli PIX

| | | |
|-------------|---|--|
| 100Mb/s | ● | Zapalona: 100 Mb/s Zgaszona: 10 Mb/s |
| FDX | ● | Zapalona: pełen duplex Zgaszona: półduplex |
| LINK | ● | Zapalona: interfejs przekazuje ruch Zgaszona: interfejs nie przekazuje ruchu |
| ACT (Tył) | ● | Zapalona: Sieć przekazuje ruch Zgaszona: Brak ruchu sieciowego |
| POWER | ● | Zapalona: Urządzenie ma zasilanie Zgaszona: Brak zasilania |
| NETWORK | ● | Migająca: Co najmniej jeden interfejs przekazuje ruch Zgaszona: Żaden z interfejsów nie przekazuje ruchu |
| ACT (Przód) | ● | Zależne od modelu PIX-a Migająca: Obraz został załadowany Zapalona: Podstawowe urządzenie w parze „failover” Zgaszona: Zapasowe urządzenie w parze „failover” |

Jak widać na rysunku 11.3, każda z diod może znajdować się w jednym z trzech stanów: zapalona, zgaszona, migająca — każdy ze stanów wskazuje inny stan danego parametru. Diody ACT zasługują na szczególną uwagę, mogą się one znajdować tak z przodu, jak i z tyłu obudowy firewalla. W przypadku niektórych modeli, jak np. PIX 506 i PIX 506E, dioda ACT, która jest umieszczona z przodu obudowy miga, gdy do pamięci flash został pomyślnie załadowany obraz systemu operacyjnego — przy rozwiązywaniu problemów ma to znaczenie istotne. W przypadku modeli wyższej klasy dioda ACT wskazuje na funkcję, jaką dany PIX pełni w obsłudze ciągłości dostępu — jeśli jest zgaszona, to firewall stanowi urządzenie zapasowe w stanie czuwania, gdy jest zapalona — firewall stanowi urządzenie podstawowe. Informacje te mogą być użyteczne w przypadku konieczności określenia, czy kabel „failover” jest sprawny i dobrze podłączony.

Podczas rozruchu firewalla PIX realizowany jest test POST (ang. *power-on self test*). Wyniki tego testu stanowią podstawowe informacje, pozwalające na określenie sprawności PIX-a. Do omówienia tego zagadnienia posłuży nam listing przedstawiony poniżej:

```
CISCO SYSTEMS PIX-501
Embedded BIOS Version 4.3.200 07/31/01 15:58:22.08
Compiled by morlee
16 MB RAM
```

```
PCI Device Table.
Bus Dev Func VendID DevID Class      Irq
00 00 00 1022 3000 Host Bridge
00 11 00 8086 1209 Ethernet    9
00 12 00 8086 1209 Ethernet   10
```

```
Cisco Secure PIX Firewall BIOS (4.2) #6: Mon Aug 27 15:09:54 PDT 2001
Platform PIX-501
Flash=E28F640J3 @ 0x3000000
```

```
Use BREAK or ESC to interrupt flash boot.
Use SPACE to begin flash boot immediately.
Reading 1536512 bytes of image from flash.
```

```
#####
16MB RAM
Flash=E28F640J3 @ 0x3000000
BIOS Flash=E28F640J3 @ 0xD8000
mcwa i82559 Ethernet at irq 9  MAC: 0008.e317.ba6b
mcwa i82559 Ethernet at irq 10 MAC: 0008.e317.ba6c
```

```
-----
          ||      ||
          ||      ||
          |||     |||
    ...:|||||:~::~:|||||:~::~:
      c i s c o S y s t e m s
    Private Internet eXchange
-----
```

Cisco PIX Firewall

Cisco PIX Firewall Version 6.2(2)

Licensed Features:

```
Failover:      Disabled
VPN-DES:       Enabled
VPN-3DES:      Disabled
Maximum Interfaces: 2
Cut-through Proxy: Enabled
Guards:        Enabled
URL-filtering: Enabled
Inside Hosts:  10
Throughput:    Limited
IKE peers:     5
```

***** Warning *****

Compliance with U.S. Export Laws and Regulations - Encryption.

***** Warning *****

Copyright (c) 1996-2002 by Cisco Systems, Inc.
Restricted Rights Legend

```
.....
Cryptochecksum(unchanged): 38a9d953 0ee64510 cb324148 b87bdd42
Warning: Start and End addresses overlap with broadcast address.
outside interface address added to PAT pool
Address range subnet is not the same as inside interface
```

Na początku rozruchu prezentowane jest oznaczenie modelu firewalle — jest to informacja szczególnie istotna w przypadku obsługi zdalnej. Proszę zwrócić uwagę na fakt, iż prezentowana jest też wersja podstawowego systemu wejścia-wyjścia PIX-a (BIOS), który jest wykorzystywany do pierwotnego rozruchu systemu. Tu jest to wersja 4.3.200. Informacja ta jest ważna w przypadku, gdy w pamięci flash nie zostanie odnaleziony żaden obraz zasadniczego systemu operacyjnego (PIX OS) — wykorzystywany jest właśnie BIOS.

Po zakończeniu procedur POST ładowany jest system operacyjny z pamięci flash, chwili tej odpowiada wiersz `Reading 1536512 bytes of image from flash`. Proces rozruchu dostarcza wielu informacji o platformie sprzętowej PIX-a. W przykładzie widać, iż ten konkretny egzemplarz ma 16 MB pamięci RAM — tak jak wcześniej wspomniano, liczba ta stanowi jeden ze wskaźników, które charakteryzują wydajność zapory. W celu zweryfikowania poprawności obrazu systemu operacyjnego sprawdzana jest jego suma kontrolna. To samo zachodzi dla BIOS PIX-a. Sumy kontrolne kodu są sprawdzane w celu ochrony przed załadowaniem i uruchomieniem uszkodzonego kodu.

Podczas ładowania PIX OS wyszukuje podłączone interfejsy — w tym przypadku znaleziono dwa interfejsy Ethernet, wyświetlane są ich adresy MAC, określane są numery przerwań, na których pracują.

Informacje prezentowane w dalszych fazach rozruchu są również bardzo cenne — często posiadanie ich pozwala uniknąć czasu zmarnowanego na bezowocną frustrację. Określana jest wersja systemu operacyjnego — w tym przypadku jest to 6.2(2). Co ważne — przedstawiane są informacje określające dostępność poszczególnych funkcji systemu. Tu np. oferowana jest obsługa sieci VPN na podstawie szyfrowania DES, nie jest już jednakże obsługiwane szyfrowanie 3DES. Liczba hostów sieci wewnętrznej ograniczona jest do 10, a liczba węzłów korzystających z IKE — do 5. Przykładowy firewall obsługuje funkcje Cut-Through Proxy i filtrowanie adresów URL.

Ostatnich kilka wierszy wygenerowanych podczas rozruchu firewalle może być pomocnych w zidentyfikowaniu błędów konfiguracji — dotyczą one procesu jej ładowania. Komunikaty te powinny zostać przestudiowane, gdyż może się okazać, że konieczne jest wprowadzenie poprawek w konfiguracji. W przedstawionym przykładzie istnieje pewien problem ze sposobem, w jaki zostały określone adresy IP. Można tu również stwierdzić, że na interfejsie sieci wewnętrznej realizowana jest translacja PAT. Informacje tego rodzaju, w zależności od sytuacji — mogą być mniej lub bardziej istotne.

Po zakończeniu procesu rozruchu dalszej weryfikacji sprzętu można dokonywać za pomocą odpowiednich poleceń PIX-a. Do określania sprzętowej konfiguracji PIX-a i kontroli stanu funkcji odpowiadających pierwszej warstwie modelu OSI wykorzystuje się tylko kilka poleceń. Poniższy listing prezentuje rezultat polecenia `show version`. Wyświetlone dane stanowią podstawowe informacje o firewallu, takie jak np. liczba i rodzaj interfejsów, numery seryjne itd. Wiele z nich pokrywa się z informacjami prezentowanymi podczas rozruchu, dotyczą one tak oprogramowania zapory, jak i jego platformy sprzętowej:

```
PIX1> show version
```

```
Cisco PIX Firewall Version 6.2(2)  
Cisco PIX Device Manager Version 2.1(1)
```

```
Compiled on Fri 07-Jun-02 17:49 by morlee
```

```
PIX1 up 23 secs
```

```
Hardware: PIX-501, 16 MB RAM, CPU Am5x86 133 MHz  
Flash E28F640J3 @ 0x3000000, 8MB  
BIOS Flash E28F640J3 @ 0xffffd8000, 128KB  
0: ethernet0: address is 0008.e317.ba6b, irq 9  
1: ethernet1: address is 0008.e317.ba6c, irq 10
```

```
Licensed Features:  
Failover: Disabled  
VPN-DES: Enabled  
VPN-3DES: Disabled  
Maximum Interfaces: 2  
Cut-through Proxy: Enabled  
Guards: Enabled  
URL-filtering: Enabled  
Inside Hosts: 10  
Throughput: Limited  
IKE peers: 5
```

```
Serial Number: 406053729 (0x1833e361)  
Running Activation Key: 0xc598dce8 0xe775fc1c 0xbd76cee8 0x3f41e74b  
Configuration last modified by at 06:28:16.000 UTC Thu Feb 7 2036
```

Pierwsza część listingu wyświetlonego za pomocą polecenia `show version` zawiera informację o wersji załadowanego i uruchomionego systemu operacyjnego oraz informację o wersji oprogramowania PIX Device Manager (PDM). Kolejne dane wskazują czas, jaki upłynął od uruchomienia firewalla — zdarza się, że informacja ta jest ważna. Kolejno wyświetlane informacje obejmują model, wielkość dostępnej pamięci oraz rodzaj i prędkość pracy procesora. Prezentowana jest wielkość obu pamięci flash. Dane te są istotne, gdyż dają możliwość określenia, czy sprzęt jest obciążony zgodnie ze swoim przeznaczeniem. Następnie przedstawiane są informacje o interfejsach — w tym egzemplarzu obecne są dwa interfejsy Ethernet. Proszę zwrócić uwagę, iż są tu wyszczególnione ich adresy MAC. Ostatnia część wyświetlonych danych zawiera numer seryjny urządzenia, klucz aktywacji, który posłużył do aktywacji obrazu systemu, oraz datę ostatniej modyfikacji konfiguracji PIX-a². Choć informacje te nie są aż tak istotne podczas rozwiązywania problemów, to jednak mogą być wymagane przy ewentualnym kontakcie z centrum pomocy technicznej Cisco (ang. *Cisco TAC*).

Podczas rozwiązywania problemów polecenie `show version` powinno stanowić jedno z pierwszych (o ile nie pierwsze) poleceń wykorzystywanych do pozyskania informacji o funkcjonalnych komponentach badanej zapory. Znajomość ich jest istotna, jeszcze zanim zostaną podjęte jakiegokolwiek działania naprawcze — w innym przypadku może zdarzyć się np. tak, że cenny czas zostanie roztrwoniony na uruchamianie funkcji, która przez dany firewall nie jest w ogóle obsługiwana. Proszę zwrócić uwagę, iż polecenie `show version` prezentuje informacje o adresach MAC poszczególnych interfejsów — często są one konieczne do rozwiązywania problemów z odzwierciedlaniem adresów fizycznych na sieciowe, tj. adresów warstwy drugiej na adresy trzeciej warstwy modelu OSI.

² Tu — jak widać — konfiguracja pochodzi z dalekiej przeszłości :-) — *przyp. tłum.*

Polecenie `show interface`, którego działanie zaprezentowano poniżej, daje informacje odnoszące się do różnych warstw — podczas rozwiązywania problemów jest ono wielce przydatne. Prezentuje ono szczegółowe informacje o poszczególnych interfejsach. Podobnie jak w przypadku routerów Cisco, polecenie to pozwala sprawdzić stan każdego interfejsu i określić, czy jest on w pełni sprawny. Oczywiście prezentowana jest nazwa każdego z interfejsów.

```
PIX1# show interface
interface ethernet1 "inside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0008.e317.ba6c
  IP address 10.10.2.1, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit full duplex
  4 packets input, 282 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  4 packets output, 282 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 babbles, 0 late collisions, 0 deferred
  0 lost carrier, 0 no carrier
  input queue (curr/max blocks): hardware (128/128) software (0/1)
  output queue (curr/max blocks): hardware (0/1) software (0/1)
```

Dane, które prezentuje polecenie `show interface`, mają nieocenioną wartość diagnostyczną. Jednakże gdy nie wiadomo, jak je zinterpretować, to w całej swojej obfitości są bezużyteczne. Jedną z rzeczy, które pozwala określić polecenie `show interface`, jest nazwa interfejsu i adres sieci przypisane do danego interfejsu fizycznego. W przedstawionym powyżej przykładzie interfejsowi `ethernet1` przypisano nazwę `inside` (do sieci wewnętrznej). Podczas rozwiązywania problemów konieczne może okazać się sprawdzenie, czy rzeczywiście do interfejsu `ethernet1` przyłączona jest założona dla niego sieć. Prezentowany jest tu też adres MAC (`0008.e317.ba6c`) i rodzaj interfejsu (`ethernet`).

Maksymalna wielkość jednostki transmisji, MTU (ang. *maximum transmission unit*), stanowi maksymalny rozmiar pakietu, który może być przesłany danym interfejsem bez konieczności fragmentowania go. Jeśli rozmiar pakietu jest zbyt duży, to pakiet ten zostanie podzielony na części i przesłany w większej liczbie ramek. Problemy, jakie powstają w związku z MTU, dotyczą przypadków, w których MTU różnych urządzeń nie jest zgodne, tzn. gdy MTU urządzenia wysyłającego ramkę jest większe do MTU urządzenia odbierającego. Polecenie to prezentuje też informacje o trybie pracy interfejsu, tzn. czy pracuje on w trybie duplex, czy w trybie półduplex. Jak wspomniano już wcześniej — informacje te można również określić, obserwując odpowiednie diody LED. Niezgodności trybu pracy, istniejące np. pomiędzy zaporą i przełącznikiem sieciowym, stanowią problem dość powszechny. Interfejsy obu urządzeń powinny pracować z tą samą prędkością i w tym samym trybie.

Kolejne informacje prezentowane przez polecenie `show interface` to informacje statystyczne, dotyczące pakietów, które przeszły przez interfejs. Dostępne są informacje o tym, ile pakietów zostało wysłanych, ile odebranych, ile łącznie zawierały bajtów. Podczas rozwiązywania problemów warto zwrócić uwagę na licznik `no buffer`, określa on, ile razy nastąpiła sytuacja, w której nadchodzące pakiety nie mogły zostać zbuforowane w celu przetworzenia. Jeżeli wartość tego licznika jest większa od zera, to do interfejsu napływa więcej pakietów, niż może być przetworzonych — interfejs jest przeciążony. W takim

przypadku interfejs powinien zostać wymieniony na bardziej wydajny albo ruch napływający do tego interfejsu powinien zostać w jakiś sposób ograniczony. Każdy z interfejsów ma nadto następujące liczniki, związane z występowaniem błędów i ramek ogłoszeniowych:

- **broadcasts** — liczba ramek, które wysłano na sprzętowy adres broadcast.
- **runts** — liczba ramek, które były mniejsze od dopuszczalnego rozmiaru (Ethernet — 64 bajty).
- **giants** — liczba ramek, które były większe od dopuszczalnego rozmiaru (Ethernet — 1518 bajtów).
- **CRC** — liczba ramek, które nie przeszły testu CRC. Jeśli występują takie błędy, to należy sprawdzić okablowanie — ich źródłem mogą być np. przesłuchy.
- **frame** — liczba ramek, w przypadku których stwierdzono błąd w rodzaju ramki. Jeśli występują takie błędy, to należy się upewnić, że wszystkie komunikujące się urządzenia mają określony ten sam rodzaj ramki.
- **overrun** — liczba ramek, które nie mogły zostać zbuforowane przez interfejs ze względu na przeciążenie.
- **ignored** — licznik niewykorzystywany.
- **abort** — licznik niewykorzystywany.
- **collisions** — liczba ramek, które spowodowały kolizje. W przypadku łączy półdupleks występowanie kolizji jest zjawiskiem naturalnym, tak więc ich obecność nie zawsze wskazuje na jakieś problemy.
- **underrun** — liczba ramek, które nie mogły zostać wysłane, gdyż przeciążony PIX nie dostarczył danych na czas.
- **babbles** — licznik niewykorzystywany.
- **late collisions** — liczba ramek, w przypadku których kolizja wystąpiła z opóźnieniem (Ethernet — 64 bajty). W przeciwieństwie do zwykłych kolizji, występowanie opóźnionych kolizji świadczy o jakimś problemie. Źródła problemu należy upatrywać w złym okablowaniu, np. w którym przekroczone dopuszczalne długości kabli, albo w zbyt dużej liczbie wzmacniaków.
- **deferred** — liczba ramek, które zostały wstrzymane ze względu na aktywność łącza. W ogólnym przypadku jest to skutek zatłoczonej sieci — interfejs jest zmuszony odraczać transmisje do chwili znalezienia dostępnego okna, w którym mógłby umieścić ramkę. Problem ten może prowadzić do nadmiernego wykorzystania dostępnych buforów — dane muszą być przechowywane do chwili transmisji.
- **lost carrier** — liczba przypadków, gdy sygnał nośny został utracony. Powodem takiego stanu rzeczy może być wadliwe okablowanie albo np. wyłączony przełącznik.
- **no carrier** — licznik niewykorzystywany.



W przypadku interfejsów pracujących w trybie pełen duplex kolizje, opóźnione kolizje i odroczone ramki nigdy nie powinny występować.

Liczniki `output queue` i `input queue` określają liczbę bajtów, które zostały zakolejkowane do wysłania i — odpowiednio — odebrania. Liczniki te stanowią migawkę stanu buforów w chwili wprowadzenia polecenia. Jeśli firewall jest zmuszony do obsługi ruchu w ilości większej, niż jest to dla niego założone, to miejsce w buforach zostanie wyczerpane, gdyż ich rozmiar jest ograniczony. Po nadejściu do interfejsu ramki dane są umieszczane w jego buforze sprzętowym (wejściowym). Następnie dane są przekazywane do bufora systemowego (wejściowego) w postaci bloków danych o określonym rozmiarze. W przypadku sieci Ethernet będą to bloki 1550-bajtowe, w przypadku 66 MHz Gigabit Ethernetu będą to bloki o wielkości 16384 bajtów. Następnie przetworzone już dane przekazywane są do bufora sprzętowego (wyjściowego) odpowiedniego interfejsu. Jeśli kolejka ta jest pełna, to dane są ponownie umieszczane w buforze systemowym (wyjściowym).

W przypadku obu buforów systemowych — jeśli określona maksymalna liczba bloków zostanie zwiększona w celu obsługi ruchu o silniejszym natężeniu i nastąpi przeciążenie interfejsu, to jedyną radą jest wymiana interfejsu na szybszy, ewentualnie, jeśli to możliwe — można również zredukować natężenie ruchu.

Rozwiązywanie problemów z okablowaniem

Jeśli problem nie został wyeliminowany, a istnieje już pewność, że wszystkie komponenty sprzętowe PIX-a funkcjonują poprawnie — następną czynnością jest sprawdzenie okablowania. W przeciwieństwie do routerów, które umożliwiają obsługę szerokiej gamy standardów okablowania, firewall PIX dysponuje względnie małymi możliwościami. Omówienie okablowania w kontekście rozwiązywania problemów z PIX-em ograniczone więc będzie do kabli Ethernet i kabla „failover”.

Niektóre modele PIX-a, dostarczane z wersjami oprogramowania do 5.3, obsługują również sieci Token Ring i FDDI. Firma Cisco przestała jednakże sprzedawać PIX-y obsługujące tego rodzaju sieci — FDDI w czerwcu 2001 r., a Token Ring w sierpniu tego samego roku. Począwszy od odpowiednio czerwca i sierpnia 2006 r. — firma Cisco nie będzie udzielać już żadnego wsparcia dla tych sieci. W książce tej temat okablowania Token Ring i FDDI nie będzie podjęty.

Niezależnie od tego, jakiego typu okablowanie sprawia problemy, podejście do ich rozwiązania powinno być konstruktywne. Kilka istotnych kwestii związanych z okablowaniem zebrano w tabeli 11.2. Przeanalizowanie wszystkich wymienionych tu zagadnień daje gwarancję, że żaden mały problem — który może być źródłem większego — nie zostanie pominięty.

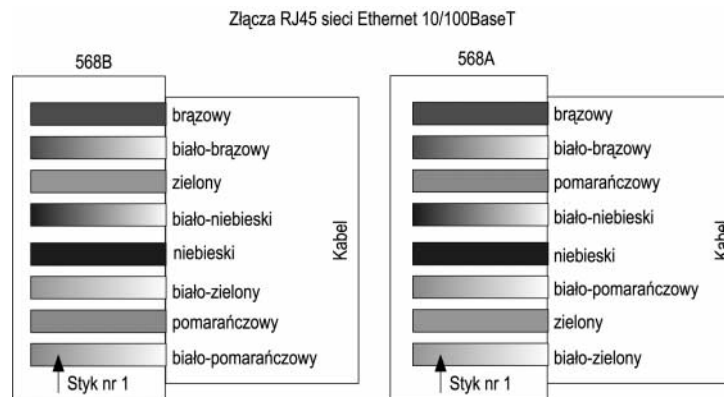
Wszystkie firewalle PIX obsługują sieć Ethernet 10/100 Mb/s, wykorzystanie Gigabit Ethernetu jest możliwe tylko w przypadku PIX 525 i PIX 535. Rozważając wydajności, jakie oferują poszczególne modele PIX-a, taki stan rzeczy jest usprawiedliwiony. Słabsze modele byłyby przeciążone po dodaniu choćby jednego interfejsu Gigabit Ethernet.

Tabela 11.2. Najważniejsze zagadnienia związane z weryfikacją okablowania

| Problem | Sposób weryfikacji |
|--|---|
| Niewłaściwy kabel podłączony do niewłaściwego interfejsu. | Należy sprawdzić, czy do danego gniazda i portu przyłączony jest prawidłowy kabel. |
| Niewłaściwy koniec kabla podłączony do niewłaściwego interfejsu. | Tylko w przypadku kabla „failover”: Koniec kabla oznaczony jako „primary” powinien być podłączony do urządzenia podstawowego, drugi koniec — do zapasowego. |
| Niewłaściwy rodzaj kabla. | Kable skrośne i kable „rollover” powinny być podłączone do odpowiednich portów. |
| Nieprawidłowy rozkład sygnałów na złączu. | Należy sprawdzić kolory przewodów i posłużyć się testerem kabli. |
| Uszkodzony kabel. | Kabel należy sprawdzić testerem albo na urządzeniach, które są w pełni sprawne. |

W chwili pisania tego tekstu PIX 535 zapewnia wydajność rzędu 9 Gb/s przy braku szyfrowania, PIX 525 — 360 Mb/s, PIX 515 — 188 Mb/s, PIX 506 — 20 Mb/s, a PIX 501 — 10 Mb/s. Rozpatrując sieć na poziomie warstwy fizycznej, zasadniczą kwestią będzie to, czy wykorzystywany jest właściwy rodzaj kabli Ethernet oraz czy ich złącza są podłączone w odpowiedni sposób. Odpowiedni układ styków kabli Ethernet i Fast Ethernet przedstawia rysunek 11.4.

Rysunek 11.4.
Rozkład połączeń
kabla Ethernet



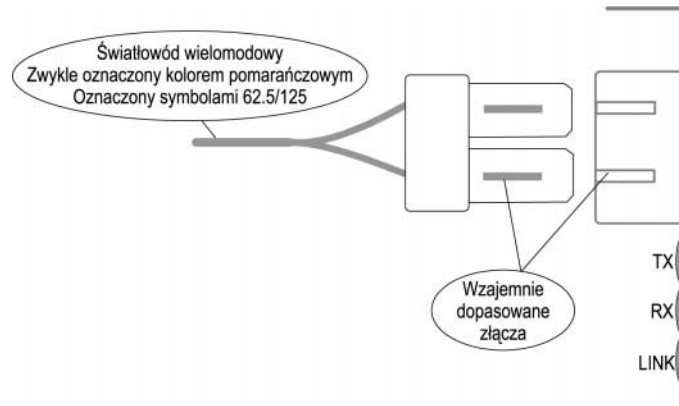
Zasadniczo dla 10/100 Mb/s Ethernet istnieją dwa standardy podłączania wtyków RJ45: TA568A i TA 568B, oba przedstawiono na rysunku 11.4. Typowy kabel Ethernet składa się z czterech par przewodów. Przewody każdej pary są ze sobą skręcone, ma to na celu minimalizację przesłuchów i innych interferencji. Nadto istotny jest sposób, w jaki przewody podłączone są do złączy. Zgodność sposobu podłączenia poszczególnych przewodów do wtyków RJ45 z przedstawionymi standardami gwarantuje, że poziom przesłuchów będzie minimalny.

Sprawdzanie kabla może być procesem względnie prostym — na rynku dostępna jest cała gama urządzeń przeznaczonych właśnie do tego celu, poczynawszy od tych najprostszych — sprawdzających prawidłowość połączeń wtyków, do urządzeń bardzo zaawansowanych — badających również i fizyczne parametry kabla. Czas zaoszczędzony dzięki zakupowi takiego urządzenia stanowi o szybkim zwrocie poniesionych nakładów.

Pierwszym krokiem weryfikacji miedzianego kabla Ethernet 10/100 Mb/s powinny być jego oględziny — nie powinien mieć żadnych uszkodzeń zewnętrznych. Następnie należy sprawdzić rozkład połączeń, powinien on wyglądać jak na rysunku 11.4. Jeśli wszystko się zgadza i kabel nie ma uszkodzeń, to należy go sprawdzić za pomocą testera. Większość testerów kabli pozwala na określenie schematu kabla — niewłaściwe podłączenie gniazd jest problemem dość częstym. Jeśli mimo pozytywnych rezultatów testów kabel sprawia kłopoty — należy go wymienić. Istnieją wszakże niewielkie szanse na to, że podczas produkcji kabla w rdzeniu któregoś z przewodów metal został pomieszany z tworzywem sztucznym, co zaburza ruch elektronów. Zawsze gdy nie dysponuje się wystarczająco dobrym testerem, a kabel jest podejrzany, to należy go wymienić.

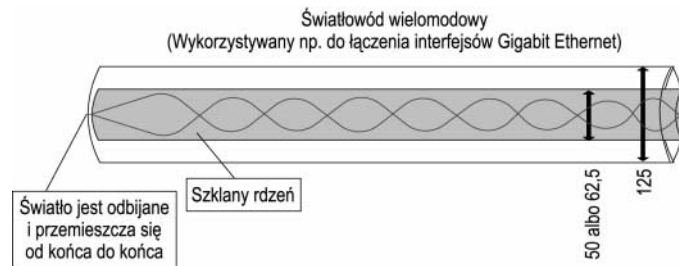
Modele PIX 525 i PIX 535 dają możliwość korzystania z Gigabit Ethernetu w trybie pełen duplex. Interfejsy Gigabit Ethernet PIX-a wyposażone są w złącza SC i obsługują światłowody wielomodowe. Jak pokazano na rysunku 11.5 — jedno z włókien światłowodu jest przeznaczone do nadawania, drugie do odbioru. W przypadku niektórych rodzajów złączy należy uważać, by włókna nie zostały podłączone odwrotnie. Wykorzystywane w firewallach Cisco złącza SC³ uniemożliwiają tego typu pomyłki — wtyk zakańczający światłowód można włożyć do gniazda na karcie interfejsu tylko w jeden sposób.

Rysunek 11.5.
Złącze SC



Swobodne użytkowanie światłowodów wymaga pewnej wiedzy. Ogólnie światłowody dzielą się na jednomodowe (ang. *single-mode*) i wielomodowe (ang. *multi-mode*). Do interfejsów Gigabit Ethernet PIX-a można podłączać tylko światłowody wielomodowe, w których światło załamuje się tak, jak to przedstawiono na rysunku 11.6.

Rysunek 11.6.
Uproszczona
budowa światłowodu
wielomodowego



³ Tzw. duplex-SC — *przyp. tłum.*

Producenci światłowodów zwykle stosują się do ustalonych standardów w sposób ścisły. Na zewnętrzną warstwę światłowodu nanoszone są oznaczenia, które dają możliwość m.in. identyfikacji rodzaju światłowodu oraz średnicy rdzenia optycznego i jego płaszczu, podawanych w mikronach. Światłowody jednomodowe zwykle oznaczane są kolorem żółtym, światłowody wielomodowe — kolorem pomarańczowym. Informacji tej nie należy traktować jako pewnika, gdyż niektórzy producenci światłowodów oznaczają swoje wyroby innymi kolorami. Interesujące nas światłowody wielomodowe mają grubość rdzenia 50 albo 62,5 mikrona. W przypadku obu światłowodów otulina rdzenia ma tę samą średnicę, wynosi ona 125 mikronów.

Podobnie jak w przypadku skrętki, tak w przypadku światłowodu — kabel może być sprawdzony odpowiednim testerem. W przeciwieństwie do przewodów miedzianych, przewody światłowodowe są bardzo czułe na czynniki mechaniczne. Niewielkie rozbieżności charakterystyki światłowodu od zaleceń standardów uniemożliwiają jego wykorzystanie, wszelkie zmiany w strukturze światłowodu są zmianami nieodwracalnymi. Jeśli przygotowany kabel nie działa, to problem też zazwyczaj wynika ze sposobu, w jaki zostały zarobione końcówki włókna (złe obcięcie, niewłaściwe wypolerowanie itp.). W takich właśnie sytuacjach przydaje się dobry tester kabli. Jeśli nie posiada się wiedzy technicznej i doświadczenia w zarabianiu światłowodów — to zadanie to należy zlecić profesjonalistom.

Rozwiązywanie problemów z komunikacją

Aby firewall mógł realizować swoje funkcje, musi mieć możliwość komunikacji z odpowiednimi węzłami sieci. Możliwość przekazywania pakietów od źródła do celu może być ograniczana przez rozmaite czynniki, takie jak np. dostępność trasy, możliwość realizacji translacji adresów, obecność odpowiedniej konfiguracji list dostępu itd. Translacja adresów jest tu szczególnie istotna, gdyż wszystkie adresy zawarte w pakietach przesyłanych z sieci wewnętrznej przed przekazaniem tych pakietów do sieci zewnętrznej muszą być poddane translacji adresów.

Administrator PIX-a powinien mieć w nawyku zwyczaj, by po każdej zmianie konfiguracji translacji adresów, list dostępu, ścieżek, czy jakichś innych funkcji obsługi ruchu, które zależą od translacji adresów — wykonywać polecenie `clear xlate`, które czyści tablicę translacji. Ponieważ w przypadku firewalli PIX translacja adresów jest obowiązkowa, tak więc będzie to konieczność, która zachodzi praktycznie podczas prawie dowolnej rekonfiguracji PIX-a. Pozostawienie starych wpisów w tablicy translacji może prowadzić do nieoczekiwanego zachowania zapory.

Proszę pamiętać o sposobie, w jaki współpracują interfejsy o różnych poziomach bezpieczeństwa. Choć domyślnie ruch pochodzący z interfejsu o wyższym poziomie bezpieczeństwa, a skierowany do interfejsu o poziomie niższym jest przekazywany, to jednak do faktycznej realizacji przekazywania konieczne jest dokonanie translacji adresów. Przekazywanie ruchu pochodzącego z interfejsów o niższym poziomie bezpieczeństwa, a skierowanego do interfejsów o poziomie wyższym wymaga tak odpowiedniej konfiguracji list dostępu albo ścieżek, jak i właściwej translacji adresów.

Nie sposób przecenić znaczenie regularnego sprawdzania dziennika nadzoru — zapewnia on bieżący, uaktualniany w czasie rzeczywistym raport o aktywności firewalle i wszystkich błędach, które występują na zaporze. Informacje te często mogą być niezastąpionym kluczem do usunięcia usterki, a przydatność ich jest nieoceniona na każdym etapie diagnozowania. W przypadku usuwania problemów z listami dostępu i translacją adresów stanowią pomoc szczególną. Na przykład jeśli host, który znajduje się w sieci przyłączonej do interfejsu o niższym poziomie bezpieczeństwa próbuje nawiązać połączenie TCP z hostem, który znajduje się w sieci przyłączonej do interfejsu o wyższym poziomie bezpieczeństwa, a odpowiednia translacja adresów jest określona, jednakże nie ma żadnej ścieżki ani listy dostępu, to w dzienniku nadzoru będzie utworzony następujący wpis:

```
106001: Inbound TCP connection denied from x.x.x.x/x to x.x.x.x/x
```

Wpis taki stanowi pierwszą wskazówkę, że realizacja założonego dostępu wymaga skonfigurowania odpowiedniej listy dostępu albo ścieżki. W sytuacji, gdy realizowana jest podobna próba dostępu, a nie został określony sposób translacji adresów — w dzienniku nadzoru zostanie odnotowane:

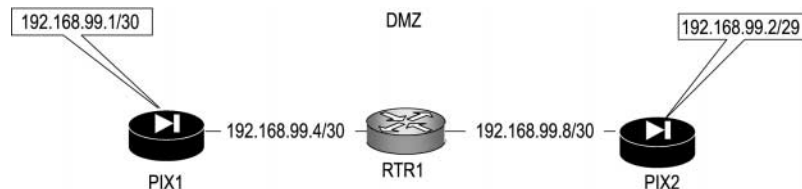
```
305005: No translation group found for...
```

Więcej informacji na temat różnych generowanych przez PIX-a komunikatów znaleźć można pod adresem www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/syslog/pixemsgs.htm.

Weryfikacja adresowania

Podobnie jak w przypadku każdego urządzenia IP, tak w przypadku PIX-a — jeśli podstawowe informacje o adresowaniu nie zostaną określone poprawnie, to czas poświęcony na usuwanie usterek w konfiguracji routingu, list dostępu i translacji adresów będzie czasem straconym. Podkreślenie kwestii poprawnego adresowania nie może być przecenione, bez niego PIX nie będzie działał poprawnie. Rysunek 11.7 przedstawia sieć, w której są dwa firewalle — PIX1 i PIX2 oraz router — RTR1.

Rysunek 11.7.
Problem z adresowaniem IP



Problem zilustrowany na rysunku 11.7 dotyczy sposobu adresowania w sieci LAN o nazwie DMZ. Sieć ta łączy obie zapory, interfejs prowadzący do tej sieci na firewallu PIX1 ma adres 192.168.99.1/30, a na firewallu PIX2 — 192.168.99.2/29. Informacje te można pozyskać za pomocą polecenia `show ip address`. Proszę zwrócić uwagę na różnice, zostały one wyróżnione w poniższych listingach:

```
PIX1# show ip address
System IP Addresses:
  ip address outside 192.168.99.5 255.255.255.252
  ip address DMZ 192.168.99.1 255.255.255.252
```

```
Current IP Addresses:
  ip address outside 192.168.99.5 255.255.255.252
  ip address DMZ 192.168.99.1 255.255.255.252

PIX2# show ip address
System IP Addresses:
  ip address outside 192.168.99.9 255.255.255.252
  ip address DMZ 192.168.99.2 255.255.255.248
Current IP Addresses:
  ip address outside 192.168.99.9 255.255.255.252
  ip address DMZ 192.168.99.2 255.255.255.248
```

Rozwiązanie problemu jest w tym przypadku proste — wystarczy dokonać korekty maski na zaporze PIX2. Podobnie jak to ma miejsce na routerach Cisco, adresy przypisane do interfejsów można również sprawdzić za pomocą polecenia `show interface`. Rezultat tego polecenia prezentuje poniższy listing:

```
PIX1# show interface
interface ethernet0 "DMZ" is up, line protocol is up
Hardware is i82559 ethernet, address is 0008.e317.ba6b
IP address 192.168.99.1, subnet mask 255.255.255.252
MTU 1500 bytes, BW 100000 Kbit half duplex
  2 packets input, 258 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  11 packets output, 170 bytes, 0 underruns, 0 unicast rpf drops
  0 output errors, 0 collisions, 0 interface resets
  0 babbles, 0 late collisions, 0 deferred
  0 lost carrier, 0 no carrier
  input queue (curr/max blocks): hardware (128/128) software (0/1)
  output queue (curr/max blocks): hardware (0/2) software (0/1)
```

Niezależnie od wykorzystywanej metody diagnostyki, weryfikacja adresów przypisanych do interfejsów sieciowych powinna stanowić pierwszy krok rozwiązywania problemów z komunikacją IP. Brak poprawnego adresowania uniemożliwia działanie wszystkich funkcji, które podczas swego funkcjonowania z niego korzystają. Niezależnie od tego, czy będą skonfigurowane poprawnie — jeśli będą problemy z adresowaniem, to funkcje te i tak działać nie będą. Należy pamiętać, iż ruch sieciowy musi przejść co najmniej przez dwa interfejsy PIX-a, oba z nich muszą posiadać odpowiednie adresy IP.

Weryfikacja trasowania

Sytuacja, w której pakiety nie mogą dotrzeć do miejsca przeznaczenia, stanowi pierwszą oznakę występowania problemów z trasowaniem. Choć rozwiązanie tego rodzaju problemów często jest dość trudne, to jednakże pracę można sobie ułatwić — należy obrać metodę polegającą na stopniowej eliminacji możliwych przyczyn. Firewall PIX obsługuje zarówno routing statyczny, jak i dynamiczny. Obsługa trasowania dynamicznego jest obecna tylko w postaci obsługi protokołu RIP, routing statyczny jest realizowany przy wykorzystaniu skonfigurowanych tras statycznych. Rozważania na temat weryfikacji trasowania rozpoczniemy od omówienia różnych opcji trasowania dostępnych na PIX-ie oraz sposobu, w jaki te opcje na siebie oddziałują.



Moduł FWSM 1.1 przeznaczony dla przełączników z serii Catalyst 6500 daje również możliwość trasowania dynamicznego przy wykorzystaniu protokołu OSPF. W tym rozdziale protokół OSPF nie jest omawiany.

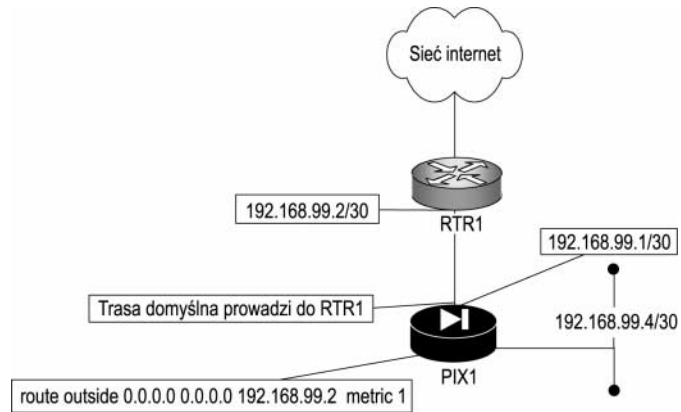
Po pierwsze, przyjrzyjmy się sposobom, w jakie określa się konfigurację routingu na PIX-ie. Jako pierwsze należy rozpatrzyć trasy domyślne i trasy statyczne, a następnie — określone za pomocą RIP trasy dynamiczne. W przypadku najprostszej konfiguracji firewall ma skonfigurowaną tylko trasę domyślną. Na przykład:

```
route outside 0.0.0.0 0.0.0.0 192.168.99.2 metric 1
```

Polecenie to określa, że wszelki ruch, który nie jest skierowany do żadnej z sieci wewnętrznych, będzie kierowany do węzła 192.168.99.2. Weźmy przykład z rysunku 11.8 — zakładając, że przedstawiona trasa stanowi jedyną skonfigurowaną trasę domyślną, to cały ruch, który nie jest skierowany do interfejsów sieci prywatnej, będzie przekazywany do routera RTR1. W przypadku sieci, której struktura jest tak prosta, jak ta na rysunku 11.8, wszystko będzie funkcjonować poprawnie. Jak jednakże będzie wyglądać sytuacja, gdy ta sama konfiguracja dotyczy będzie sieci przedstawionej na rysunku 11.9?

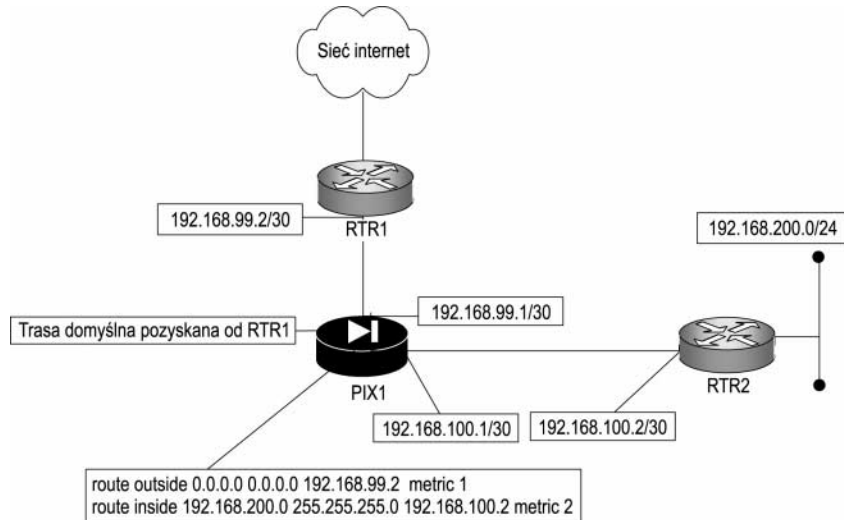
Rysunek 11.8.

Przykład sieci, w której wykorzystano trasę domyślną



Rysunek 11.9.

Trasy statyczne



Jak wynika z rysunku 11.9 — ruch z zapory PIX1 skierowany do sieci 192.168.200.0/24 powinien być przekazywany do RTR2. Jeśli wykorzystywana byłaby jedynie trasa wspomniana wcześniej, to wszelki ruch skierowany do sieci 192.168.200.0/24 byłby przekazywany do routera RTR1 i do celu nigdy by nie dotarł. Rozwiązanie problemu polegałoby tu na dodaniu na firewallu PIX1 odpowiedniej trasy statycznej, prowadzącej do sieci 192.168.200.0/24. W tym celu należałoby wprowadzić:

```
route inside 192.168.200.0 255.255.255.0 192.168.100.2 metric 2
```

Prócz trasowania statycznego, firewall PIX ma również możliwość trasowania dynamicznego przy wykorzystaniu protokołu RIP wersja 1. i RIP wersja 2. W przeciwieństwie do routerów Cisco, gdzie zakres dostępnych opcji obsługi RIP jest bardzo szeroki, zbiór poleceń PIX-a jest tu skromny:

```
[no] rip <nazwa_interfejsu> default
[no] rip <nazwa_interfejsu> passive
[no] rip <nazwa_interfejsu> version {1 | 2}
[no] rip <nazwa_interfejsu> authentication {text | md5} <ciąg_znaków_klucza>
<id_klucza>
```

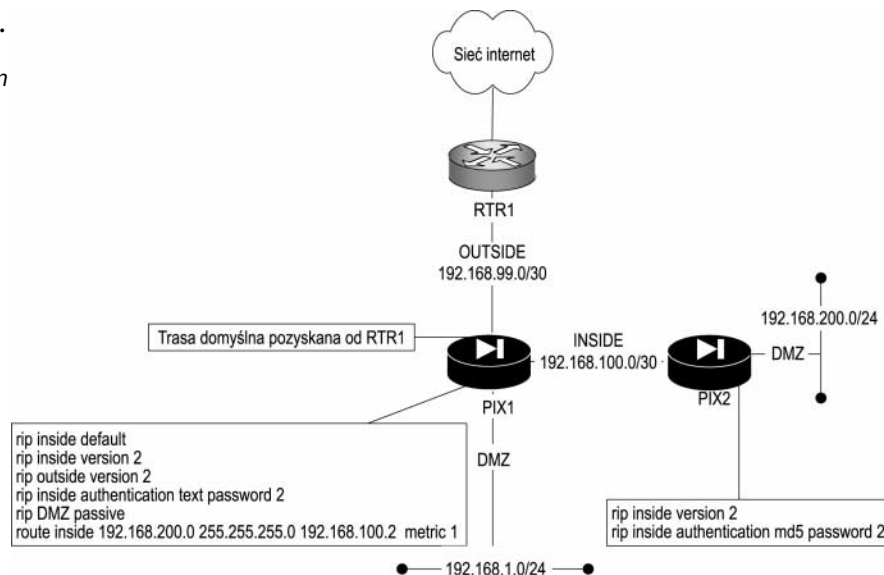
Nie będziemy się w tym miejscu nadmiernie rozwodzić nad aspektami korzystania z protokołu RIP. Słowo kluczowe `default` określa, iż firewall będzie rozgłaszać z danego interfejsu trasę domyślną. Słowo kluczowe `passive` precyzuje, że na danym interfejsie PIX powinien obsługiwać wymianę tras w sposób bierny, tj. pobierać trasy samemu, jednakże ich nie rozgłaszać. Słowo kluczowe `version` jest wykorzystywane do określenia wersji protokołu, którym ma się posługiwać zapora. Ponadto w konfiguracji można określić, że węzły, które wymieniają trasy za pomocą RIP, mają dokonywać wzajemnego uwierzytelnienia, w takim przypadku konfiguracja PIX-a wymaga posłużenia się słowem kluczowym `authentication`. Obsługę protokołu RIP konfiguruje się dla każdego interfejsu osobno.

Statyczne trasowanie do sieci 192.168.200.0/24 z poprzedniego przykładu zastąpmy protokołem RIP wersja 2. Sytuację przedstawia rysunek 11.10. Proszę zauważyć, iż wprowadzona zmiana pozwala PIX-owi na lepszą adaptację do zmian w strukturze sieci.

W przypadku firewalli PIX protokół RIP nie ogłasza tras pomiędzy poszczególnymi interfejsami. W sieci przedstawionej na rysunku 11.10 zapora PIX1 nasłuchuje uaktualnień tras pochodzących z sieci DMZ 192.168.1.0/24. W rezultacie PIX1 jest w stanie odpowiednio trasować pakiety skierowane do tej sieci. W konfiguracji protokołu RIP dla interfejsu sieci DMZ użyto słowa kluczowego `passive`, tak więc do tej sieci trasy nie będą rozgłaszane. Co więcej — pozyskane z tej sieci informacje o trasach do innych sieci nie będą rozgłaszane do zapory PIX2 i routera RTR2. Ograniczenie to wynika ze sposobu obsługi protokołu RIP przez firewalle PIX. Aby je obejść, na PIX1 należy dodać trasę domyślną, która prowadzi do PIX2 (co w przykładowej konfiguracji już zrobiono), a na routerze RTR1 określić trasę statyczną do sieci DMZ chronionej firewallem PIX1. Jedyne trasy, które będą rozgłaszane przez PIX1, to trasy domyślne i trasy do sieci, które są przyłączone bezpośrednio do jego interfejsów — router RTR1 i zapora PIX2 będą więc mieć informacje o trasach do wszystkich sieci chronionych firewallem PIX1. Pakiety przekazywane przez PIX2, a skierowane do dowolnych sieci za interfejsem sieci DMZ zapory PIX1 również będą docierać do celu — określona na PIX2 trasa domyślna prowadzi do PIX1.

Rysunek 11.10.

Trasowanie
z wykorzystaniem
protokołu RIP



Wspomniane ograniczenie może być koniecznością i zaletą. Wszystkie adresy przechodzące przez interfejs sieci zewnętrznej firewalle PIX1 powinny być poddawane translacji adresów. Tak więc router RTR1 nie musi znać tras do sieci znajdujących się za interfejsem DMZ firewalle PIX1 — adresy te i tak są poddawane translacji do adresu publicznego, który to właśnie RTR1 wykorzystuje do przekazywania pakietów do PIX1.

W sieci, którą przedstawiono na rysunku 11.10, jest problem, który jest dość oczywisty. Widać, iż sposoby uwierzytelniania wykorzystywane przez obie zapory są wzajemnie niedopasowane. Zapora PIX1 do uwierzytelniania używa haseł przesyłanych tekstem jawnym, a zapora PIX korzysta z szyfrowania MD5. Choć na obu zaporach podano to samo hasło, to protokół RIP funkcjonować tu nie będzie — różnica w określeniu sposobu szyfrowania sprawi, że zapory nie będą mogły się nawzajem uwierzytelnić, a co za tym idzie — nie będą mogły dokonać wymiany tablic routingu.

Inny potencjalny problem, który należy rozważyć, to niezgodność wersji protokołu RIP. W protokole RIP wersja 1. trasy są dystrybuowane za pomocą rozgłaszania pod adres 255.255.255.255, w protokole RIP wersja 2. — również za pomocą rozsyłania grupowego pod adres 224.0.0.9. Ponadto wersja 2. umożliwia uwierzytelnianie, wersja 1. — nie. Podczas rozwiązywania problemów z trasowaniem wszystkie urządzenia, na których jest używany RIP, należy zweryfikować pod kątem zgodności co do wersji tego protokołu. Jeżeli używany jest RIP wersja 2., to należy upewnić się, że określono ten sam sposób szyfrowania i to samo hasło. Obsługa RIP wersja 2. została wprowadzona w wersji 5.1 oprogramowania PIX-a. Należy więc pamiętać, iż wcześniejsze wersje systemu nie będą współpracować z urządzeniami używającymi RIP wersja 2. Obsługa rozsyłania grupowego dla RIP wersja 2. została wprowadzona w wersji 5.3 oprogramowania zapory. Wersje wcześniejsze obsługują tylko i wyłącznie rozgłaszanie.

Po krótkim przedstawieniu sposobu, w jaki firewalle PIX realizują trasowanie, możemy skupić się na rozwiązywaniu problemów właściwych sytuacjom, w których określony host sieci jest nieosiągalny czy też żadna prowadząca do niego trasa nie jest dostępna.

Podczas rozwiązywania tego typu problemów należy posłużyć się poleceniami, takimi jak `show route`, `show rip` i `ping`. Osiągalność danego hosta można sprawdzić za pomocą polecenia `ping`. Jeśli dany host jest nieosiągalny, to za pomocą polecenia `show route` należy sprawdzić, czy istnieje jakaś trasa prowadząca do danej sieci. Polecenie `show rip` można wykorzystać w celu weryfikacji konfiguracji trasowania dynamicznego. Składnia polecenia `ping` wygląda następująco:

```
ping [<nazwa_interfejsu>] <adres>
```

Na przykład:

```
PIX1# ping 192.168.99.2
  192.168.99.2 response received - 20 ms
  192.168.99.2 response received - 20 ms
  192.168.99.2 response received - 20 ms
```

Jeśli istnieje wątpliwość, co do tego, czy PIX ma jakąś trasę domyślną, statyczną albo określoną za pomocą protokołu RIP, to należy sprawdzić tablicę routingu. Oto przykład użycia polecenia `show route`:

```
PIX1# show route
  outside 192.168.99.0 255.255.255.252 192.168.99.1 1 CONNECT static
  inside 192.168.100.0 255.255.255.252 192.168.100.1 1 CONNECT static
  DMZ 192.168.1.0 255.255.255.0 192.168.1.1 1 CONNECT static
```

W tym przypadku host 192.168.99.2 jest położony w sieci przyłączonej bezpośrednio do interfejsu sieci zewnętrznej. W celu zweryfikowania konfiguracji protokołu RIP należy wprowadzić polecenie `show rip`. Jeśli dokona się porównania konfiguracji określonej na obu przykładowych zaporach, rezultat będzie następujący:

```
PIX1# show rip
  rip inside default
  rip inside version 1
  rip outside version 2
  rip inside authentication text haslo1 2
  rip DMZ passive
```

```
PIX2# show rip
  rip inside default
  rip inside version 1
  rip outside version 1
  rip inside authentication md5 haslo2 2
  rip DMZ passive
```

Widoczne są tu różnice w określeniu wersji protokołu, sposobie uwierzytelniania, hasła. W rezultacie protokół RIP pomiędzy firewallami PIX1 i PIX2 nie będzie funkcjonować. Po poprawieniu konfiguracji mogłaby wyglądać następująco:

```
PIX1# show rip
  rip inside default
  rip inside version 2
  rip outside version 2
  rip inside authentication md5 haslo2 2
  rip DMZ passive
```

```
PIX2# show rip
  rip inside default
  rip inside version 2
```

```

rip outside version 2
rip inside authentication md5 haslo2 2
rip DMZ passive

```

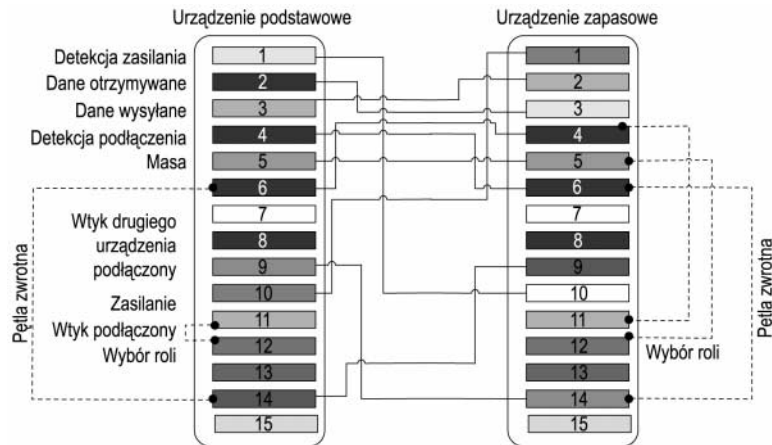
Rozważania na temat protokołu RIP zamknijemy przedstawieniem polecenia `clear rip`, które można wykorzystać, gdy zaistnieje potrzeba wyłączenia obsługi tego protokołu. Polecenie `clear rip` usuwa z konfiguracji wszystkie zawarte w niej polecenia `rip`.

Kabel „failover”

Zapory PIX wyposażone są w funkcję obsługi ciągłości dostępu (ang. *failover*). Polega ona na tym, że całość konfiguracji i operacji danego firewalla jest duplikowana na firewallu zapasowym, w razie awarii firewalla podstawowego jego funkcje przejmuje firewall zapasowy. Obsługa ciągłości dostępu w typowym przypadku wymaga połączenia obu firewallei odpowiednim kablem. Sposób podłączenia kabla określa, które z urządzeń ma pełnić rolę firewalla podstawowego, a które z nich rolę firewalla zapasowego.

Znajomość budowy kabla „failover” stanowi część wiedzy wymaganej do sprawnego rozwiązywania problemów z firewallami PIX. Schemat tego kabla przedstawiono na rysunku 11.11. Jeśli obsługa ciągłości dostępu nie działa, to należy zbadać kabel. Schemat kabla określony za pomocą testera powinien odpowiadać schematowi z rysunku 11.11.

Rysunek 11.11.
Schemat kabla „failover”



Wszystkie przewody przedstawione na powyższym rysunku pełnią jakąś funkcję. Rozróżnienie pomiędzy firewallem podstawowym i zapasowym opiera się na badaniu połączenia styku 12. (wybór roli). W złączu firewalla podstawowego styk 12. jest połączony ze stykiem 11. (podłączony). W złączu firewalla zapasowego styk 12. jest połączony ze stykiem 5. (masa). Znajomość schematu kabla daje nie tylko możliwość sprawdzenia posiadanego kabla, ale również — jeśli zajdzie taka potrzeba — budowy własnego.

Weryfikacja translacji adresów

Firewall PIX daje możliwość translacji adresów. Komunikacja hostów sieci wewnętrznej z hostami sieci zewnętrznej, jak i vice versa — wymaga translacji adresów sieciowych.


```
PIX1# show nat
nat (dmz) 0 192.168.1.10 255.255.255.255 0 0
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
nat (dmz) 99 0.0.0.0 0.0.0.0 0 0
PIX1# show global
global (outside) 99 192.168.99.4-192.168.99.254 netmask 255.255.255.0
global (outside) 1 192.168.99.3 netmask 255.255.255.0
```

Jak wynika z wyświetlonego polecenia `nat (dmz) 0...` — adres serwera z sieci DMZ, tj. 192.168.1.10, nie jest poddawany translacji. Polecenie `nat (dmz) 99...` określa, że wszystkie pozostałe adresy sieci DMZ powinny być przekształcane. Polecenia `global` określają dwie pule publicznych adresów IP, przeznaczonych do wykorzystania na cele translacji adresów. Sama translacja jest określona w poleceniach `nat`, w których umieszczone są odpowiednie identyfikatory pul adresów publicznych. Pulę wykorzystywaną do translacji NAT określa polecenie `global (outside) 99...`, polecenie `global (outside) 1...` zawiera natomiast pojedynczy adres IP, który jest używany do realizacji translacji PAT. Praktycznie rozpatrzenie wyników poleceń `show nat` i `show global` powinno wystarczyć do stwierdzenia, czy translacja jest skonfigurowana poprawnie. Po poprawieniu ewentualnych błędów konfiguracji (najczęściej są to błędy powstałe podczas wprowadzania poleceń, w szczególności w adresach IP), jej działanie warto sprawdzić w praktyce. Do weryfikacji komunikacji pomiędzy hostami należy wykorzystać polecenie `show conn detail`:

```
PIX1# show conn detail
1 in use, 1 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, D - DNS, d - dump,
       E - outside back connection, f - inside FIN, F - outside FIN
       G - group, H - H.323, I - inbound data, M - SMTP data,
       O - outdound data, P - inside back connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP RPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, U - up
TCP outside:192.168.11.11/24 dmz:192.168.99.2/80 flags UIO
```

Z powyższego listingu wynika, iż pewna stacja robocza z sieci zewnętrznej ustanowiła połączenie z serwerem HTTP (80. port TCP), który znajduje się w sieci DMZ. Proszę zwrócić uwagę, iż połączenie zostało ustanowione z wykorzystaniem publicznego adresu IP serwera (192.168.99.2), a nie z wykorzystaniem adresu prywatnego (192.168.1.2), który nie jest osiągalny z sieci zewnętrznej. Mamy tu ustanowione połączenie, ale czy naprawdę zachodzi translacja adresów? Aby to sprawdzić, należy posłużyć się poleceniem `show xlate detail`:

```
PIX1# show xlate detail
1 in use, 1 most used
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
       o - outside, r - portmap, s - static
TCP NAT from DMZ:192.168.1.2/80 to outside:192.168.99.2/80 flags ri
```

Polecenie to wyświetla bieżącą listę aktywnych translacji. Jak widać na przytoczonym listingu, w połączeniu hosta sieci zewnętrznej z serwerem WWW odpowiednia translacja jest dokonywana: adres 192.168.1.2 jest zamieniany na 192.168.99.2. Przedstawiona weryfikacja poprawności translacji adresów jest szczególnie istotna właśnie w przypadkach, gdy pewne hosty sieci wewnętrznej muszą być dostępne z sieci zewnętrznej.

Istnieje jeszcze jedno polecenie, które okazuje się użyteczne podczas rozwiązywania problemów z translacją adresów. Jest to polecenie z grupy `debug`, tak więc ze względu na oszczędność zasobów firewalla jego użycie powinno być ograniczane. Polecenie to można wykorzystywać dwójako: do śledzenia i dekodowania wymienianych pomiędzy hostami pakietów albo do określania adresów, które wymagają translacji ze względu na konieczność udostępnienia określonych zasobów. Druga z wymienionych możliwości wymaga pełniejszego wyjaśnienia. Zakładając, że nie znamy adresu hosta, któremu należy umożliwić dostęp — przechwycenie informacji o próbie nawiązania połączenia z określonym hostem (serwerem) sieci wewnętrznej byłoby pomocne. Polecenie `debug packet` daje obitą ilość informacji, jego składnia wygląda następująco:

```
debug packet <nazwa_interfejsu> [src <adres_źródła> [netmask <adres_źródła_maska>]]
[dst <adres_celu> [netmask <adres_celu_maska>]] [[proto icmp] | [proto tcp [sport
<port_źródła>] [dport <port_celu>]] | [proto udp [sport <port_źródła>] [dport
<port_celu>]] [rx | tx | both]
```

Wracając do przykładowego serwera WWW, polecenie umożliwiające pozyskanie adresów hostów, które podejmują próby nawiązania połączenia z tym serwerem, wyglądałoby następująco:

```
PIX1(config)# debug packet outside src 0.0.0.0 netmask 0.0.0.0 dst 192.168.99.2
netmask 255.255.255.0 rx
```

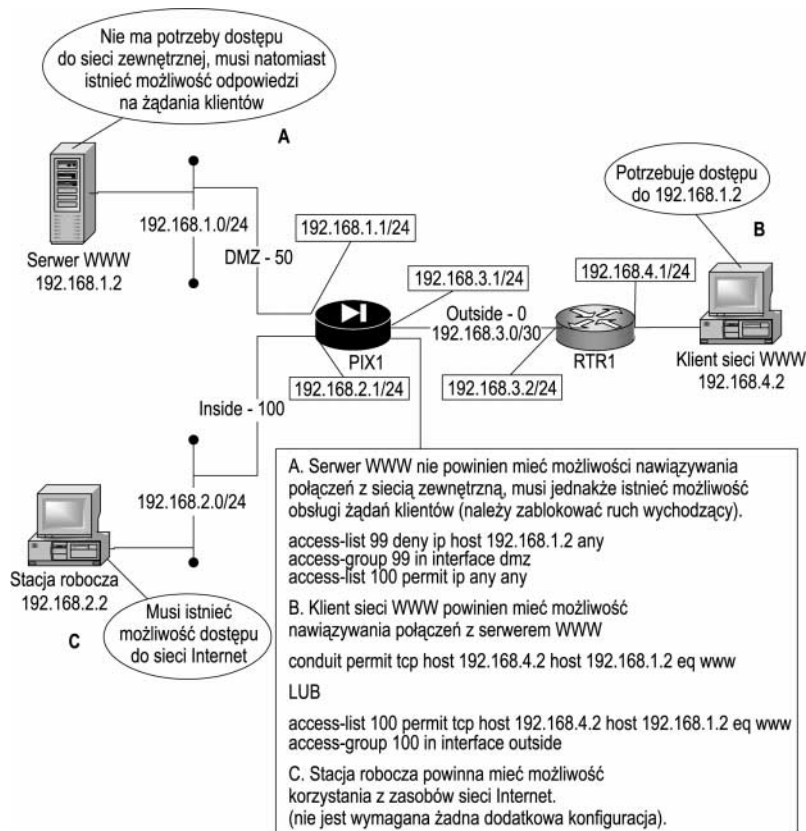
Polecenie to będzie uruchamiać przechwytywanie pakietów, które przychodzą do interfejsu sieci zewnętrznej i są skierowane pod publiczny adres serwera WWW. Ponieważ nie wiemy dokładnie, jakiego rodzaju protokół będzie wykorzystywany w połączeniu, tak więc nie został on określony w poleceniu. Po przechwyceniu ruchu, na podstawie pozyskanych danych można określić niezbędne parametry translacji adresów, którą należy skonfigurować.

Weryfikacja dostępu

Realizacja kontroli dostępu poprzez firewall PIX może być zrealizowana na kilka sposobów. W tej części rozdziału omówimy część z nich, rozpatrzmy też pewne metody pozwalające na ich monitorowanie i weryfikację poprawności ich działania. Domyślnie, jeśli tylko jest skonfigurowana odpowiednia translacja adresów, firewall PIX umożliwia dostęp w przypadku połączeń inicjowanych z sieci przyłączonej do interfejsu o wyższym poziomie bezpieczeństwa skierowanych do sieci przyłączonej do interfejsu o niższym poziomie bezpieczeństwa. Możliwość dostępu w kierunku odwrotnym musi być określona w sposób jawny, za pomocą list dostępu albo ścieżek.

Polecenie `conduit` charakteryzuje się funkcjami zbliżonymi do działania list dostępu. Jest ono wykorzystywane do umożliwiania przekazywania ruchu z interfejsu o niższym poziomie bezpieczeństwa do interfejsu o poziomie wyższym. Kilka najczęstszych scenariuszy realizacji dostępu przedstawiono na rysunku 11.13. Klient sieci WWW (poziom bezpieczeństwa 0) chce uzyskać dostęp do serwera WWW (poziom bezpieczeństwa 50), w domyślnej polityce bezpieczeństwa PIX-a tego typu ruch jest blokowany. Stacja robocza z sieci wewnętrznej (poziom bezpieczeństwa 100) potrzebuje dostępu do zasobów sieci Internet. Na rysunku przedstawiono również odpowiednią konfigurację, która realizuje założone cele — poszczególne przypadki oznaczono literami A, B i C. Założono tu, iż translacja adresów została już poprawnie określona i funkcjonuje, dzięki temu będzie można od razu zająć się istotą omawianego tematu. Użyte adresy określono na potrzeby omówienia tematu — założmy, że są one odpowiednio przekształcane.

Rysunek 11.13.
Różne scenariusze wymagające konfiguracji dostępu



Serwer WWW nie powinien mieć możliwości nawiązywania połączeń z hostami spoza sieci DMZ, powinien mieć jednakże możliwość obsługi żądań nadchodzących od klienta WWW z sieci zewnętrznej. Aby zapewnić realizację powyższych założeń, należy utworzyć listę dostępu, która uniemożliwi hostowi 192.168.1.2 wszelki dostęp do wszelkich zasobów, listę tę należy przypisać do interfejsu sieci DMZ. Następnie należy utworzyć ścieżkę, która będzie pozwalać hostowi o adresie 192.168.4.2 na dostęp do usług WWW (80. port TCP) świadczonych przez serwer 192.168.1.2. Alternatywnie, jak pokazano na rysunku — można również utworzyć odpowiednią listę dostępu. Obsługa list dostępu została wprowadzona w wersji 5.1 oprogramowania firewalle PIX. Należy pamiętać, że firma Cisco zaleca, by nie mieszać list dostępu ze ścieżkami. Co istotne — listy dostępu mają przed ścieżkami pierwszeństwo. Listy dostępu umożliwiają jedynie filtrację ruchu, który *napływa* do danego interfejsu, określanego za pomocą polecenia `access-group`.

Stacja z sieci wewnętrznej (przypadek C) musi mieć możliwość dostępu do zasobów sieci Internet. Interfejs sieci wewnętrznej ma przypisany poziom bezpieczeństwa 100, najwyższy możliwy. Jak już niejednokrotnie wspomniano — ruch z interfejsów o wyższym poziomie bezpieczeństwa skierowany do interfejsów o poziomie niższym jest domyślnie przepuszczany, po inicjalizacji połączenia ruch zwrotny jest również przepuszczany. W przypadku rozpatrywanej stacji roboczej ruch zachodzi właśnie pomiędzy tak określonymi interfejsami, tak więc żadna dodatkowa konfiguracji nie jest tu wymagana.

O problemach z brakiem dostępu świadczy nieosiągalność danych hostów. Ponieważ mechanizmy kontroli dostępu, takie jak listy dostępu i ścieżki, ściśle zależą od translacji adresów, tak więc w przypadku problemów w pierwszej kolejności należy sprawdzić właśnie funkcjonowanie translacji. Dopiero po weryfikacji działania translacji adresów można zająć się problemami z konfiguracją dostępu. Najczęstsze źródła tych problemów to nieprawidłowości powstałe podczas wprowadzania poleceń, istnienie konfiguracji list dostępu albo ścieżek, która jest zbyt czy też niewystarczająco restrykcyjna, błędy w określeniach adresów IP, przypisanie listy dostępu do niewłaściwego interfejsu. Do zweryfikowania konfiguracji dostępu wykorzystać można kilka poleceń, które przedstawiamy poniżej.

Ścieżki umożliwiają dostęp z sieci o niższym poziomie bezpieczeństwa do sieci o poziomie wyższym. Jedynym poleceniem, które daje możliwość weryfikacji konfiguracji ścieżek, jest polecenie `show conduit`. Na przykład:

```
PIX1# show conduit
conduit permit tcp host 192.168.4.2 host 192.168.1.2 eq www (hitcnt=3)
```

Przedstawiona ścieżka umożliwia hostowi 192.168.4.2 dostęp do serwera WWW o adresie 192.168.1.2. Od czasu wprowadzenia list dostępu w wersji 5.1 oprogramowania PIX-a ścieżki są stopniowo przez nie wypierane. Jeśli istnieje taka konieczność — całość konfiguracji ścieżek, tj. poleceń `conduit`, można usunąć poleceniem `clear conduit`, które w tym wypadku należy wprowadzić w trybie konfiguracji. Wprowadzenie w trybie uprzywilejowanym `clear conduit counters` powoduje wyzerowanie liczników użycia wszystkich ścieżek (`hitcnt`).

W przypadku list dostępu liczba poleceń, które można wykorzystać podczas rozwiązywania problemów, jest większa. Weryfikację skonfigurowanych list dostępu umożliwia polecenie `show access-list`:

```
PIX1# show access-list
access-list 99: 2 elements
access-list 99 deny ip host 192.168.1.2 any (hitcnt=1)
access-list 99 permit ip any any (hitcnt=0)
access-list 100 permit tcp host 192.168.4.2 host 192.168.1.2 eq www (hitcnt=5)
```

Powyższe polecenie odzwierciedla konfigurację firewalla z rysunku 11.13. Proszę pamiętać, iż działanie list dostępu ogranicza się wyłącznie do ruchu, który napływa do interfejsu. Następnym krokiem po upewnieniu się, że listy dostępu zostały określone prawidłowo, powinna być weryfikacja tego, czy listy dostępu zostały przypisane do odpowiednich interfejsów. W tym celu należy skorzystać z polecenia `show access-group`. Na przykład:

```
PIX1# show access-group
access-group 99 in interface dmz
access-group 100 in interface outside
```

Słowo kluczowe `in` jest tu obowiązkowe, jego zadaniem jest przypomnienie, iż lista dostępu tylko filtruje ruch, który napływa do interfejsu. Do rozwiązywania problemów z listami dostępu można również wykorzystać polecenia `debug`. W tym przypadku monitorowane są wszystkie zdarzenia dotyczące wszystkich list dostępu, możliwość monitorowania tylko wybranej listy dostępu nie jest możliwa. Liczba danych, które powstają po wprowadzeniu polecenia `debug access-list`, może być bardzo duża, w szczególności

gdy firewall obsługuje ruch o dużym natężeniu. Podobnie jak to ma miejsce w przypadku innych poleceń debug, polecenie `debug access-list` powinno więc być wykorzystywane w sposób oszczędny, tylko wtedy, gdy chodzi o pozyskanie jakichś konkretnych informacji. Polecenie to przydaje się np. wtedy, gdy konieczne jest sprawdzenie, czy dana lista filtruje określony ruch tak, jak powinna. Jego składnia wygląda następująco:

```
debug access-list {all | standard | turbo}
```

Kolejny mechanizm kontroli dostępu dają listy outbound. Firma Cisco odradza ich wykorzystanie i zaleca posługiwanie się listami dostępu. Mimo wszystko listy outbound stanowią pierwotny mechanizm kontroli dostępu na firewallach PIX i wciąż są tu obsługiwane. Listy outbound cechują dość nieporęczną składnią i ograniczone możliwości, a rozwiązywanie istniejących problemów jest w ich przypadku uciążliwe. Listy outbound zostały zaprojektowane z myślą o kontroli dostępu użytkowników sieci prywatnej do zasobów zewnętrznych, tj. ruchu wychodzącego. W niektórych sytuacjach użycie list outbound jest całkiem wygodne, tak więc sposoby rozwiązywania problemów z listami outbound są warte poznania. Składnia polecenia `outbound` wygląda następująco:

```
outbound <identyfikator_listy> {permit | deny | except} <adres_ip> [<adres_maska>
<port>[-<port>]] [tcp | udp | icmp]
```

Parametr `identyfikator_listy` stanowi unikatowy identyfikator listy. Słowa kluczowe `permit`, `deny` i `except` (które precyzuje, iż dany element listy ma stanowić wyjątek od sposobu użycia listy, który określono w przypisaniu listy do interfejsu) charakteryzują sposób obsługi danego ruchu. W przeciwieństwie do list dostępu elementy list outbound nie są przetwarzane od pierwszego do ostatniego. Każdy element listy outbound jest przetwarzany niezależnie od tego, czy dotyczy on danego ruchu, który przechodzi przez interfejs. Firma Cisco zaleca, by każda lista outbound rozpoczynała się od elementu, który blokuje cały ruch (`deny 0 0 0`), następnie należy określać przypadki, w których ruch ma przepuszczany. Sposób wykorzystania określonej listy outbound zależy od parametrów określonych w poleceniu `apply`, które przypisuje listę do wybranego interfejsu:

```
apply [(interfejs)] <identyfikator_listy> {outgoing_src | outgoing_dest}
```

Słowa kluczowe `outgoing_src` i `outgoing_dest` służą do określania sposobu interpretacji parametrów `adres_ip` i `port` zawartych w liście `outbound`, która jest przypisywana do danego interfejsu. Po wprowadzeniu `outgoing_src` parametry te będą traktowane jako określające źródło. Jeśli natomiast zostanie wprowadzone `outgoing_dest`, to parametry zawarte w liście `outbound` będą traktowane jako dotyczące celu. Zrozumienie faktu, iż w samej liście `outbound` nie określa się, czy wprowadzane parametry `adres` i `port` dotyczą celu, czy też źródła, jest istotne. Określenie to zawiera się dopiero w poleceniu `apply`. Z uwagi na ten fakt rozwiązywanie problemów z listami outbound może być kłopotliwe — choć sama lista może być określona prawidłowo, to jednak prawidłowo swoich funkcji może już nie pełnić, gdyż istnieją jakieś błędy w poleceniu `apply`. Tak więc podczas weryfikowania pracy list outbound konieczne jest również sprawdzenie prawidłowości poleceń `apply`. W przypadku, gdy danego rodzaju ruch podlega filtracji przy użyciu kilku różnych reguł, to wybierana jest reguła, która jest skojarzona z tym ruchem najprecyzyjniej — pod uwagę brane są zakresy adresów i portów. Im węższy zakres adresów i portów, tym bardziej dany element listy precyzuje rodzaj ruchu, który będzie za jego pomocą filtrowany. Jeśli określone reguły są ze sobą sprzeczne, to wybierana jest reguła, która przepuszcza dany ruch (`permit`). Oto przykład konfiguracji listy outbound, tu jest ona przypisywana do interfejsu sieci wewnętrznej:

```
PIX1(config)# outbound 99 deny 0 0 0
PIX1(config)# outbound 99 permit 0.0.0.0 0.0.0.0 1-1024 tcp
PIX1(config)# outbound 99 except 192.168.2.0 255.255.255.0
PIX1(config)# apply (inside) 99 outgoing_src
```

W przykładzie tym pierwszy element listy outbound blokuje cały ruch, drugi — umożliwia przepływ wszelkiego ruchu na portach 1 – 1024 TCP, trzeci — uniemożliwia sieci 192.168.2.0/24 dostęp do portów TCP, które zostały określone w poprzednim elemencie. Podczas przypisania listy do interfejsu posłużono się słowem kluczowym `outgoing_src`, tak więc zawarte w liście adresy i porty określają źródło.

Liczba poleceń, które pozwalają na rozwiązywanie problemów z listami outbound, jest niewielka. Przede wszystkim po każdorazowej rekonfiguracji list dostępu należy wyczyścić tablicę translacji, tj. wprowadzić polecenie `clear xlate`. Aby wyświetlić wszystkie skonfigurowane listy dostępu, należy posłużyć się poleceniem `show outbound`. Polecenie `show apply` umożliwia weryfikację poleceń `apply`, tzn. tego, czy listy zostały w odpowiedni sposób przypisane do właściwych interfejsów. List outbound nie dotyczy żadne z poleceń z grupy `debug`. Rolę starszych list outbound przejmują nowsze listy dostępu, które — tak jeśli chodzi o konfigurację, jak i o rozwiązywanie problemów — dają większe możliwości. Składnia poleceń związanych z listami dostępu jest bliższa normom przyjętym przez firmę Cisco, a obsługa filtracji jest tu prostsza i łatwiejsza do zrozumienia.

Jedna z funkcji firewala PIX nie wydaje się stanowić funkcji związanej z kontrolą dostępu, jednakże z drugiej strony — ponieważ ogranicza możliwości pewnych protokołów — nieomówienie jej mogłoby świadczyć o ignorancji. Mowa tu o analizie protokołów w warstwie aplikacji, konfigurowanej za pomocą poleceń `fixup`. W przypadku protokołów, takich jak HTTP, FTP, SMTP i innych, funkcja ta jest domyślnie włączona, a jej działanie zawęża możliwości protokołów do podstawowych funkcji określonych standardami — ma to na celu minimalizację ryzyka wykorzystania specyficznych właściwości tych protokołów do zrealizowania ataku sieciowego. Aby określić, dla których protokołów jest uruchomiona analiza w warstwie aplikacji, należy wprowadzić polecenie `show fixup`. Na przykład:

```
PIX1# show fixup
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
```

Rozwiązywanie problemów z IPsec

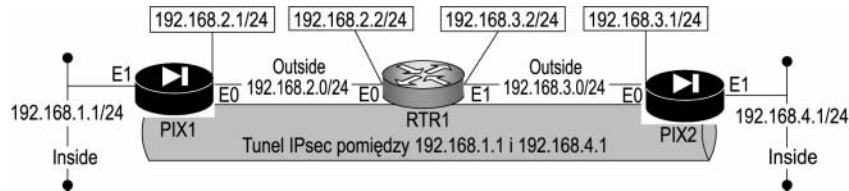
Architektura IPsec jest przez firewall PIX wykorzystywana do ustanawiania bezpiecznych tuneli VPN pomiędzy dwoma komunikującymi się hostami. Celem tworzenia tuneli VPN jest bezpieczna wymiana danych po IP. Konfiguracja IPsec dopuszcza tu różne warianty

uwierzytelniania: IKE kluczy RSA, IKE przy wykorzystaniu certyfikatów zewnętrznych, IKE kluczy predefiniowanych albo wymianę kluczy predefiniowanych bez procedur IKE (ang. *manual IPsec*). W ostatnim przypadku wystarczy po prostu określić odpowiednie hasło, które ma być wykorzystywane do uwierzytelniania przez oba komunikujące się ze sobą hosty — rozwiązanie to jest mało bezpieczne, a oparty na nim system — mało skalowalny.

Tu skoncentrujemy się na rozwiązywaniu problemów dotyczących wykorzystania IPsec z IKE kluczy predefiniowanych. Źródłami problemów z IPsec mogą być błędy w określeniu konfiguracji, nieprawidłowe parametry i klucze, różne kwestie związane z trasowaniem i adresowaniem itp. Podobnie jak w innych przypadkach — najpierw problemy należy zidentyfikować na podstawie objawów, po znalezieniu źródła problemu należy je w odpowiedni sposób wyeliminować.

Rysunek 11.14 przedstawia przykładowy tunel IPsec, który został ustanowiony pomiędzy dwoma zaporami, PIX1 i PIX2. IPsec jest dość skomplikowane — zwykle wszelkie, nawet najdrobniejsze błędy konfiguracji całkowicie uniemożliwiają jego poprawne funkcjonowanie. Pierwszą rzeczą, którą należy przyswoić, jest więc sposób konfiguracji IPsec na zaporze PIX.

Rysunek 11.14.
Przykład tunelu IPsec



Oto przykładowe konfiguracje IPsec dla tunelu przedstawionego na rysunku 11.14, analiza ich jest okazją do poznania kilku niezbędnych poleceń. Konfiguracja zapory PIX1:

```
! PIX1 Configuration snippets
nat 99 0.0.0.0 0.0.0.0
global (outside) 99 192.168.2.10-192.168.2.254 netmask 255.255.255.0
route outside 0.0.0.0 0.0.0.0 192.168.2.2
static (inside, outside) 192.168.2.10 192.168.1.1 netmask 255.255.255.255
conduit permit ip 192.168.3.0 255.255.255.0 any
isakmp enable outside
isakmp policy 99 authen pre-share
isakmp policy 99 encryption des
isakmp policy 99 group 1
isakmp policy 99 hash md5
isakmp policy 99 lifetime 9999
isakmp identity address
isakmp key cisco address 192.168.3.1
access-list 99 permit ip 192.168.0.0 255.255.252.0 any
crypto ipsec transform-set FW1 ah-md5-hmac esp-des esp-md5-hmac
crypto map FW1 1 ipsec-isakmp
crypto map FW1 2 set peer 192.168.3.1
crypto map FW1 3 match address 99
crypto map FW1 interface outside
```

Konfiguracja zapory PIX2:

```
! PIX2 Configuration snippets
nat 99 0.0.0.0 0.0.0.0
global (outside) 99 192.168.3.10-192.168.2.254 netmask 255.255.255.0
route outside 0.0.0.0 0.0.0.0 192.168.3.2
static (inside, outside) 192.168.3.10 192.168.4.1 netmask 255.255.255.255
conduit permit ip 192.168.3.0 255.255.255.0 any
isakmp enable outside
isakmp policy 99 authen pre-share
isakmp policy 99 encryption des
isakmp policy 99 group 1
isakmp policy 99 hash md5
isakmp policy 99 lifetime 9999
isakmp identity address
isakmp key cisco address 192.168.2.1
access-list 99 permit ip 192.168.0.0 255.255.252.0 any
crypto ipsec transform-set FW1 ah-md5-hmac esp-des esp-md5-hmac
crypto map FW1 1 ipsec-isakmp
crypto map FW1 2 set peer 192.168.2.1
crypto map FW1 3 match address 99
crypto map FW1 interface outside
```

Kilka kwestii wymaga tu omówienia. Przede wszystkim punkty końcowe tunelu IPsec, który jest tworzony pomiędzy zaporami, są tu określone adresami sieci wewnętrznych, nie adresami publicznymi. Choć konfiguracja taka jest poprawna, to stanowi metodę wdrażania IPsec, która nie jest zalecana przez firmę Cisco. Co więcej, użyte adresy sieci wewnętrznych są tu poddawane statycznej translacji na adresy publiczne. Prowadzi to do problemu, który polega na tym, że adres źródła zawarty w tunelowanych pakietach będzie po ich dotarciu do celu różny od adresu źródła pakietów — pakiety zostaną uznane za niepoprawne. Rozwiązanie tego problemu sprowadza się do wyeliminowania translacji adresów wykorzystywanych w komunikacji IPsec (nat 0), dodania tras, które będą prowadzić do odpowiednich hostów sieci wewnętrznych, i umożliwienia przekazywania pakietów do tych hostów.

ISAKMP

Zadaniem procedur ISAKMP (ang. *Internet Security Association and Key Management Protocol*) jest negocjacja sposobów uwierzytelniania, wymiany kluczy i szyfrowania, wymaganych do ustanowienia bezpiecznego połączenia IPsec pomiędzy hostami. Ustalone w toku działania procedur ISAKMP sposoby uwierzytelniania i zabezpieczenia stanowią wstępną konfigurację IPsec, która jest wykorzystywana podczas dalszych negocjacji i w samym toku komunikacji IPsec.

Korzystające z ISAKMP hosty ustalają za jego pomocą odpowiednie zbiory parametrów metod zabezpieczeń, które będą czynić zadość politykom bezpieczeństwa obu hostów. Parametry te obejmują sposób wymiany kluczy, uwierzytelniania i szyfrowania, takie jak np. ustawienia algorytmu Diffiego-Helmana, czy rodzaj funkcji mieszającej. Ustanowienie uwierzytelnionego i bezpiecznego kanału pomiędzy procesami ISAKMP oraz właściwa negocjacja i wymiana kluczy realizowane są za pomocą IKE. Uzgodnione poprzez ISAKMP parametry muszą być wspólne dla obu hostów, w przeciwnym razie działanie IKE będzie niemożliwe, a co za tym idzie — komunikacja IPsec nie będzie mogła być zrealizowana.

Działanie IKE może zachodzić w dwu trybach, tzw. fazach. W trybie podstawowym, tj. fazie 1. (ang. *Phase 1*), następuje negocjacja wspólnego zbioru parametrów bezpieczeństwa wymaganych do realizacji komunikacji IPsec, w toku wymiany komunikatów ustalana jest wspólna polityka bezpieczeństwa, określana wymogami ISAKMP. Po jej ustaleniu hosty mogą utworzyć bezpieczne połączenie za pomocą ISAKMP. Tryb szybki, tzw. faza 2. (ang. *Phase 2*), również służy do negocjacji wspólnego zbioru parametrów bezpieczeństwa, jednakże tryb ten i ustalone parametry nie są wykorzystywane przez ISAKMP, a np. bezpośrednio przez IPsec.

Przed rozpoczęciem wdrażania IPsec na firewallu PIX należy upewnić się, że wszystkie hosty, które będą uczestniczyć w komunikacji, są wzajemnie osiągalne. Jeśli sprzęt, sieć albo np. sposób translacji adresów uniemożliwia komunikację hostów, to problemy należy rozwiązać według wcześniej przedstawionej w tym rozdziale metodologii. Osiągalność hostów może być zweryfikowana za pomocą polecenia ping.

Konfiguracja i parametry polityki bezpieczeństwa ISAKMP mogą być zweryfikowane za pomocą kilku poleceń. Podstawową konfigurację ISAKMP można wyświetlić za pomocą polecenia `show isakmp`. Na przykład:

```
PIX1# show isakmp
isakmp enable outside
isakmp key ***** address 192.168.3.1 netmask 255.255.255.255
isakmp identity address
isakmp policy 99 authentication pre-share
isakmp policy 99 encryption des
isakmp policy 99 hash md5
isakmp policy 99 group 1
isakmp policy 99 lifetime 9999
```

Polecenia `show isakmp` i `show crypto isakmp` wyświetlają bieżącą konfigurację PIX-a. Proszę zwrócić uwagę, iż ze względów bezpieczeństwa wyświetlany klucz jest zamaskowany. Należy pamiętać, iż w toku działania ISAKMP musi zostać znaleziony zbiór wspólnych parametrów polityki bezpieczeństwa ISAKMP, tak więc przytoczone polecenia powinny posłużyć do weryfikacji zgodności polityki bezpieczeństwa na obu komunikujących się hostach (zaporach) — konieczne jest istnienie choć jednego wspólnego zbioru parametrów. Jeśli konieczne jest poznanie bardziej szczegółowych informacji na temat konfiguracji polityki bezpieczeństwa ISAKMP, to należy skorzystać z polecenia `show crypto isakmp policy`. Wyświetlone parametry stanowią dokładniejsze określenie parametrów, które są wyświetlane za pomocą `show isakmp`. Każdy z nich przedstawiony jest w dużo bardziej opisowy sposób:

```
PIX1# show crypto isakmp policy
Protection suite of priority 99
  encryption algorithm:  DES - Data Encryption Standard (56 bit Keys).
  hash algorithm:        Message Digest 5
  authentication method: Pre-Shared Key
  Diffie-Hellman group:  #1 (768 bit)
  Lifetime:              9999 seconds, no volume limit Default protection suite
  encryption algorithm:  DES - Data Encryption Standard (56 bit Keys).
  hash algorithm:        Secure Hash Standard
  authentication method: Rivest-Shamir-Adleman Signature
  Diffie-Hellman group:  #1 (768 bit)
  Lifetime:              86400 seconds, no volume limit
```

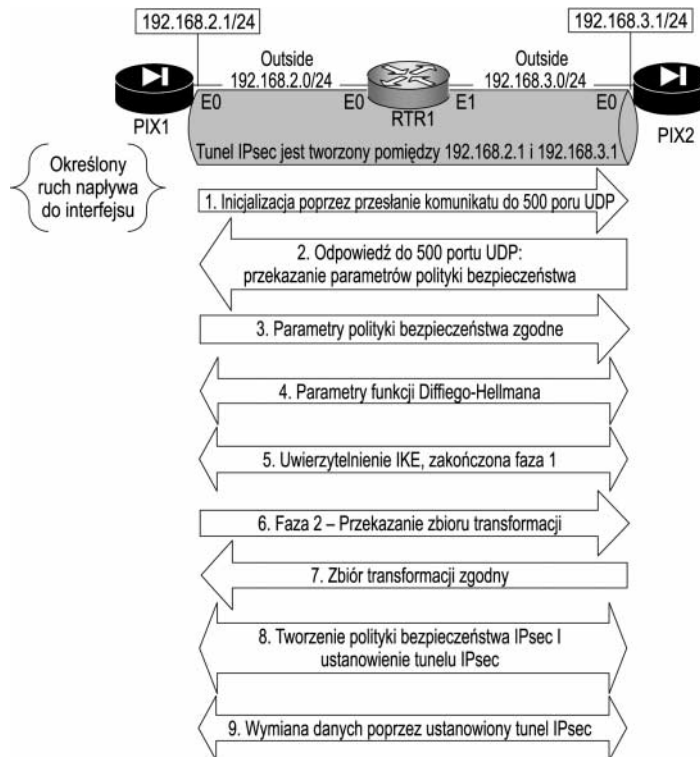
Polecenie `show crypto isakmp policy` jest o tyle użyteczne, iż prezentuje również wartości domyślne, które są wykorzystywane w przypadku, gdy w konfiguracji w sposób jawny nie określono żadnych innych.

Jeśli działanie IKE jest niemożliwe, to niemożliwa jest również komunikacja IPsec. Jedyny wyjątek ma miejsce wtedy, gdy działanie IPsec nie opiera się na IKE, tzn. gdy wymieniane są klucze predefiniowane przez użytkownika (ang. *manual IPsec*).

Proces negocjacji ISAKMP może być obserwowany po wprowadzeniu polecenia `debug crypto isakmp`. Polecenie to generuje znaczną ilość danych, tak więc powinno być wykorzystywane z rozwagą. Wyświetlane informacje przedstawiają przebieg negocjacji wspólnej polityki bezpieczeństwa (fazy 1. i 2. IKE) i samą wymianę kluczy. Proces debugowania jest uruchamiany po nadejściu odpowiedniego rodzaju ruchu do interfejsu, na którym określono dany adres wykorzystywany do komunikacji IPsec (rodzaj ruchu określony w danej mapie szyfrowania). Przykładowy przebieg procesu tworzenia tunelu IPsec przedstawiono na rysunku 11.15 (Tu podczas komunikacji oba hosty wysyłają datagramy do 500. portu UDP — wcześniej należało upewnić się, że komunikacja taka może zachodzić).

Rysunek 11.15.

Przykładowy przebieg procesu tworzenia tunelu IPsec



Proces tworzenia tunelu rozpoczyna się od weryfikacji adresów IP i par kluczy obu hostów. Inicjator wysyła własne parametry polityki bezpieczeństwa ISAKMP, odbiorca odpowiada, wysyłając parametry, które przystają do jego własnej polityki. W dalszej części pierwszej fazy IKE wymieniane są parametry algorytmu Diffiego-Hellmana oraz generowane są klucze sesji. Po zakończeniu pierwszej fazy IKE oba hosty są uwierzytelnione i mają

określony cały zbiór parametrów polityki bezpieczeństwa. Druga faza IKE przebiega przy mniejszej liczbie wymian komunikatów, negocjowane są tu parametry wykorzystywane bezpośrednio przez IPsec. Po zakończeniu fazy drugiej jest ustanawiany tunel IPsec, rozpoczyna się transmisja danych.

Najpowszechniejszy problem, związany z funkcjonowaniem ISAKMP, to różnice w predefiniowanych kluczach albo innych parametrach polityki bezpieczeństwa ISAKMP. Pierwszym krokiem, który podejmuje się w przypadku problemów z ISAKMP, jest porównanie konfiguracji obu hostów. Można to uczynić za pomocą poleceń, które zostały przedstawione wcześniej. Po upewnieniu się, iż istnieje zgodność pomiędzy parametrami obu polityk, należy wprowadzić odpowiednie polecenie `debug` i rozpocząć sesję IPsec. Dzięki bezpośredniemu wglądowi w przebieg tworzenia połączenia IPsec zlokalizowanie istniejącego błędu będzie proste.

Jeśli na obu hostach nie zostaną określone żadne wspólne parametry polityki ISAKMP albo też polityki te nie zostaną określone wcale, to w toku działania IKE zostaną wykorzystane parametry domyślne. Szyfrowanie zostanie oparte na DES, wartości funkcji skrótu będą obliczane za pomocą algorytmu SHA, uwierzytelnianie będzie realizowane za pomocą RSA, a w algorytmie Diffiego-Hellmana zostanie wykorzystana grupa 1. (768 bitów), z czasem życia 86400 sekund. Rozbieżności w definicji polityk bezpieczeństwa można stwierdzić po wprowadzeniu polecenia `show crypto isakmp sa`. Jeśli zostaną wyświetlone parametry określone jako `no state`, to znaczy to, iż wartości tych parametrów, na przykład funkcje skrótu czy klucze, nie mogły zostać uzgodnione pomiędzy obiema stronami. W takim przypadku dalsza komunikacja IPsec nie jest możliwa. Rezultaty, np. rozbieżności w parametrach funkcji skrótu, mogą oczywiście być obserwowane po wprowadzeniu `debug crypto isakmp`.

W przypadku, gdy istnieje konieczność usunięcia uzgodnionego zbioru parametrów polityki i reinicjalizacji ISAKMP, należy posłużyć się poleceniem `clear crypto isakmp`. Polecenie to może być pomocne nie tylko wtedy, gdy konieczna jest sama reinicjalizacja sesji, ale również podczas monitorowania procesu negocjacji IKE za pomocą poleceń `debug`.

IPsec

Po zakończeniu negocjacji parametrów przez ISAKMP — metod szyfrowania, uwierzytelniania i rozmiaru klucza, IPsec dysponuje informacjami niezbędnymi do utworzenia tunelu VPN. Wspomniane parametry są przez IPsec wymagane. Oba hosty, które zamierzają komunikować się za pomocą IPsec, porównują własne zbiory transformacji i określają te, które są obsługiwane przez obie strony. W ten sposób negocjowane są sposób uwierzytelniania, szyfrowania i funkcja skrótu. Jeśli obie strony nie znajdą wspólnego zbioru transformacji, to tunel nie zostanie ustanowiony.

Aby sprawdzić skonfigurowane zbiory transformacji, należy posłużyć się poleceniem `show crypto ipsec transform-set`. Proszę zauważyć, iż polecenie to pozwala na określenie, czy IPsec będzie negocjować nagłówki uwierzytelnienia (AH), sposób szyfrowania zawartości pakietów (ESP), czy też wykorzystane będą obie możliwości. Oto przykład:

```
PIX1# show crypto ipsec transform-set
```

```
Transform set FW1: { ah-md5-hmac }
  will negotiate = { Tunnel, },
  { esp-des esp-md5-hmac }
  will negotiate = { Tunnel, },
```

Istotne jest, by parametry określone w zbiorach transformacji były wspólne dla obu stron. Ruch, który ma podlegać szyfrowaniu, określany jest za pomocą tzw. map szyfrowania (ang. crypto map). Ich weryfikacji można dokonać za pomocą polecenia show crypto map. Na przykład:

```
PIX2# show crypto map
```

```
Crypto Map: "pixola" interfaces: {outside }

Crypto Map "pixola" 1 ipsec-isakmp
  Peer = 192.168.2.1
  access-list 100 permit ip 192.168.2.0 255.255.255.0 any (hitcnt=1)
  Current peer: 192.168.2.1
  Security association lifetime: 4608000 kilobytes/28800 seconds
  PFS (Y/N): N
  Transform sets={ pix. }
```

Polecenie show crypto map prezentuje informacje o adresie drugiego hosta IPsec i interfejsie, do którego dana mapa jest przypisana. W powyższym przykładzie na zaporze PIX mapa o nazwie pixola została przypisana do interfejsu sieci zewnętrznej. Ruch IPsec jest wymieniany pomiędzy zaporą PIX2 a hostem o adresie 192.168.2.1 (PIX1), szyfrowany ruch jest przepuszczany na podstawie listy dostępu o nazwie 100. Podana jest tu również informacja o tym, ile razy dana lista dostępu została wykorzystana — daje to możliwość łatwego określenia natężenia danego ruchu IPsec.

Po zweryfikowaniu, czy oba hosty dysponują wspólnym zbiorem transformacji i czy mapy szyfrowania są określone poprawnie — warto sprawdzić, czy przesyłane dane są rzeczywiście zabezpieczane. Możliwość taką daje polecenie show crypto ipsec sa. Oto przykładowy rezultat:

```
PIX1# show crypto ipsec sa
interface: outside
Crypto map tag: pixola, local addr. 192.168.2.1

local ident (addr/mask/prot/port): (192.168.2.1/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.3.1/255.255.255.0/0/0)
current_peer: 192.168.3.1
PERMIT, flags={origin_is_acl,}

#pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify 5
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress
  failed: 0
#send errors 0, #recv errors 0
local crypto endpt.: 192.168.2.1, remote crypto endpt.: 192.168.3.1
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: 3a18fca2
inbound esp sas:
spi: 0x61af4121(2451330208)
```

```

transform: esp-des esp-md5-hmac
in use settings =(Tunnel, )
slot: 0, conn id: 1, crypto map: pixola
sa timing: remaining key lifetime (k/sec): (4000159/9460)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:
inbound pcp sas:

outbound esp sas:
spi: 0x61af4121(2451330208)
transform: esp-des esp-md5-hmac
in use settings =(Tunnel, )
slot: 0, conn id: 1, crypto map: pixola
sa timing: remaining key lifetime (k/sec): (4000159/9460)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:
outbound pcp sas:

```

Rezultat tego polecenia może być, jak widać, obszerny. Crypto map tag określa tu wykorzystywaną mapę szyfrowania, local ident i remote ident określają adresy obu komunikujących się hostów. Liczniki #pkts dają bieżące informacje o liczbach pakietów, które zostały zaszyfrowane, odszyfrowane i skompresowane. Z powyższego listingu wynika, iż liczba otrzymanych, jak i wysłanych zaszyfrowanych pakietów wynosi 5. Świadczy to o poprawnym funkcjonowaniu IPsec.

Oba komunikujące się hosty są określone jako local crypto endpt i remote crypto endpt. Poniżej widoczne są wybrane parametry komunikacji. Podane jest tu MTU ścieżki i nośnika — ułatwia to stwierdzenie, czy w toku komunikacji zachodzi fragmentacja. Następnie, w części inbound, wyświetlane są informacje o schemacie obsługi ruchu przychodzącego. Parametr spi stanowi unikatowy identyfikator tunelu. W części transform prezentowany jest wykorzystywany zbiór transformacji oraz informacja o trybie IPsec (transport czy tunel). Wielkość remaining key lifetime oznacza czas i liczbę kilobitów, jakie pozostały do ponownej renegocjacji zbioru parametrów polityki bezpieczeństwa. Część outbound daje analogiczną możliwość sprawdzenia parametrów obsługi ruchu wychodzącego.

Czas i liczbę kilobitów, jakie pozostały do ponownej renegocjacji zbioru parametrów polityki bezpieczeństwa, można sprawdzić za pomocą polecenia show crypto ipsec security-association. Na przykład:

```

PIX1# show crypto ipsec security-association lifetime
Security association lifetime: 4608000 kilobytes/28800 seconds

```

Proces negocjacji sesji IPsec można obserwować po wprowadzeniu polecenia debug crypto ipsec. Jak wspomniano wcześniej, negocjacja ta zachodzi dopiero po negocjacji parametrów przez ISAKMP. Z uwagi na liczbę danych, jakie są prezentowane po wprowadzeniu debug crypto isakmp i debug crypto ipsec, polecenia te powinny być stosowane oddzielnie. Najpierw należy rozwiązywać problemy z ISAKMP, dopiero później problemy z IPsec.

W razie potrzeby sesje IPsec mogą być reinicjalizowane. Jest to przydatne wtedy, gdy dana sesja jest błędnie skonfigurowana albo gdy po prostu chce się utworzyć tunel od nowa — np. w celu rozpoczęcia procesu monitorowania ustanawiania sesji IPsec za pomocą poleceń debug. Aby wymusić ponowną negocjację wspólnego zbioru parametrów polityki bezpieczeństwa, należy wprowadzić polecenie `clear crypto ipsec sa`. Polecenie to usuwa wszystkie bieżące parametry i jeśli tylko istnieje odpowiednia mapa szyfrowania, to po nadejściu odpowiedniego ruchu nastąpi negocjacja nowego wspólnego zbioru parametrów polityki bezpieczeństwa. Polecenie `clear crypto ipsec sa` daje pewne możliwości precyzowania jego działania, np. wprowadzenie `clear crypto ipsec sa 192.168.2.1` ograniczy działanie polecenia do połączeń z hostem 192.168.2.1.

Przechwytywanie ruchu sieciowego

W wersji 6.2 PIX-a została wprowadzona bardzo użyteczna funkcja — możliwość przechwytywania i analizy ruchu sieciowego. Po wprowadzeniu polecenia `capture PIX` działa jak szperacz (*ang. sniffer*) pakietów przechodzących przez dany interfejs, który przechwytuje pakiety do ich późniejszej analizy. Przechwytywany jest zarówno ruch wychodzący, jak i przychodzący.

Przechwytywanie pakietów przechodzących przez wybrany interfejs jest bardzo pomocne podczas rozwiązywania problemów — daje możliwość precyzyjnego określenia rodzaju ruchu, który jest obsługiwany na tym interfejsie. Możliwość przechwytywania pakietów jest podczas rozwiązywania problemów z komunikacją często bardzo przydatna. Przechwycone pakiety można zanalizować pod kątem błędów w konfiguracji, np. prowadzących do niezgodności adresów IP czy problemów z IPsec i ISAKMP, takich jak niezgodność parametrów czy brak odzewu na żądanie ich przesłania. Przed wprowadzeniem tej funkcji konieczne było skorzystanie z usług specjalisty, który instalował odpowiednie urządzenia przechwytyjące pakiety. Jak wspomniano — możliwość przechwytywania pakietów została wprowadzona w wersji 6.2 oprogramowania PIX-a, jest ona dostępna tylko dla interfejsów sieci Ethernet. Składnia polecenia `capture` wygląda następująco:

```
capture <nazwa> [access-list <nazwa_listy>] [buffer <rozmiar_w_B>] [ethernet-type <rodzaj_protokołu>] [interface <nazwa_interfejsu>] [packet-length <rozmiar_w_B>]
```

Pierwszy parametr, *nazwa*, określa nazwę, jaka ma zostać przypisana danej sesji przechwytywania. W przeciwieństwie do pozostałych parametrów, które są opcjonalne — parametr *nazwa* jest wymagany. Parametr `access-list` umożliwia określenie listy dostępu, która specyfikuje przechwytywany ruch. Domyślnie przechwytywane są wszystkie pakiety IP. Parametr `buffer` umożliwia określenie rozmiaru bufora służącego do gromadzenia przechwytywanych pakietów. Maksymalny rozmiar bufora jest uzależniony od rozmiaru pamięci RAM danej zapory, domyślnie jest to 515 kB. Po wypełnieniu bufora przechwytywanie jest zatrzymywane. Parametr `ethernet-type` precyzuje rodzaj protokołu, którego ramki mają być przechwytywane. Protokół może być określany za pomocą wartości z zakresu 1 – 65535 albo za pomocą nazw skrótowych, takich jak np. `ip`, `arp`, `rarp`, `ip6` itd. Domyślnie przechwytywane są wszystkie ramki sieci Ethernet (`ethernet-type 0`). Parametr `interface` daje możliwość wyszczególnienia interfejsu, na którym ma zachodzić przechwytywanie pakietów. Parametr `packet-length` określa, ile bajtów każdego pakietu ma zostać zarejestrowanych. Zwykle w przypadku rozwiązywania problemów wystarczy kilka pierwszych bajtów pakietu (nagłówki), domyślnie PIX przechwytuje 68 bajtów. Oto przykład użycia polecenia `capture`:

```
PIX1# capture inside-traffic access-list 100 buffer 20000 interface inside
packet-length 200
```

W przykładzie tym określono, iż ma być przechwytywanych pierwszych 200 bajtów pakietów, które odpowiadają liście dostępu o nazwie 100. Rozmiar bufora, w którym będą gromadzone przechwytywane pakiety, ma wynosić 20000 bajtów.

W tym samym czasie na zaporze PIX może być uruchomionych kilka procesów przechwytywania. Aby wyświetlić bieżącą listę procesów przechwytywania, należy posłużyć się poleceniem `show capture`. Poniższy przykład prezentuje sytuację, w której równocześnie przechwytywane są pakiety na dwu różnych interfejsach:

```
PIX1# show capture
capture cap 1 interface inside
capture cap 2 interface outside
```

Aby wyczyścić bufor, w którym gromadzone są przechwytywane pakiety, ale nie zatrzymywać procesu przechwytywania, należy skorzystać z polecenia `clear capture <nazwa>`. Na przykład:

```
PIX1# clear capture cap1
```

Aby zatrzymać wybrany proces przechwytywania i wyczyścić bufor przechwytywania, należy posłużyć się poleceniem `no capture <nazwa>`. Na przykład:

```
PIX1# no capture cap2
```

Aby zatrzymać wybrany proces przechwytywania, zachowując zawartość bufora przechwytywania, należy użyć polecenia `no capture <nazwa> interface <nazwa_interfejsu>`. Na przykład:

```
PIX1# no capture cap1 interface inside
```

Wyświetlanie wyników przechwytywania

Firewall PIX daje kilka różnych możliwości zapoznania się w wynikami przechwytywania. Podstawowy wariant prezentacji wyników to wyświetlenie ich na konsoli, wyniki można również wyświetlić w oknie przeglądarki WWW. Nadto przechwycone dane można pobrać z zapory i przejrzeć w zewnętrznej aplikacji, np. programie Ethereal (www.ethereal.com) czy tcpdump (www.tcpdump.org).

Wyświetlanie na konsoli

W przypadku, gdy ruch jest przechwytywany podczas rozwiązywania problemów z zaporą PIX, najbardziej praktyczne wydaje się wyświetlenie wyników na konsoli. W przypadku, gdy wyniki przechwytywania wyświetlane są na konsoli, dobrze jest zadbać o to, by przechwytywane były tylko nagłówki pakietów (IP, TCP, itd.) — przeglądanie obszernych wyników na konsoli tekstowej może być nieco uciążliwe. Aby wyświetlić wyniki przechwytywania na konsoli, należy posłużyć się poleceniem `show capture`. Polecenie to ma następującą składnię:

```
show capture <nazwa> [access-list <nazwa_listy>] [count <liczba>] [detail] [dump]
```

Jeśli ilość przechwyconych danych jest duża, to wyniki można przefiltrować przy wykorzystaniu parametru `access-list`, w tym przypadku lista dostępu będzie ograniczać dane wyświetlane na konsoli. Parametr `count` umożliwia ograniczenie liczby wyświetlanych pakietów. Wprowadzenie słowa kluczowego `detail` powoduje, że wyświetlane będą również szczegóły dotyczące przechwyconych pakietów. Po wprowadzeniu słowa kluczowego `dump` wyniki będą prezentowane w postaci liczb szesnastkowych. Oto przykład wyników przechwytywania, które wyświetlono za pomocą polecenia `show capture`:

```
PIX1# show capture inside-traffic count 6
71 packets captured
17:29:35.648434 192.168.2.1.23 > 192.168.2.2.11002: P 942178590:942178597
(7) ack 2099017897 win 4096(fragment-packet)
17:29:35.848207 192.168.2.2.11002 > 192.168.2.1.23: . ack 942178597 win
3531(fragment-packet)
17:29:37.610258 192.168.2.2.11002 > 192.168.2.1.23: P 2099017897:
2099017898(1) ack 942178597 win 3531(fragment-packet)
17:29:37.610442 192.168.2.1.23 > 192.168.2.2.11002: . ack 2099017898 win
4095(fragment-packet)
17:29:37.610686 192.168.2.1.23 > 192.168.2.2.11002: P 942178597:942178598
(1) ack 2099017898 win 4096(fragment-packet)
17:29:37.808155 192.168.2.2.11002 > 192.168.2.1.23: . ack 942178598 win
3530(fragment-packet)
```

Proszę zauważyć, jak wzrastają numery kolejnych potwierżeń (ACK). Przedstawiony fragment to pakiety sesji Telnet pomiędzy hostami 192.168.2.1 i 192.168.2.2. Na sesję Telnet wskazuje numer portu na hoście 192.168.2.1 — 23. Jak widać, przechwytywanie pakietów stanowi bardzo użyteczną funkcję podczas rozwiązywania problemów z komunikacją.

Wyświetlanie w oknie przeglądarki WWW

Firma Cisco zadbała również, by wyniki przechwytywania można było w bezpieczny sposób przeglądać za pomocą przeglądarki WWW. W celu pobrania wyników przechwytywania w oknie przeglądarki należy wprowadzić adres URL, który wskazuje na daną zaporę PIX, a odnosi się do nazwy określonej podczas wprowadzania polecenia `capture`. Składnia tego adresu wygląda następująco:

```
https://adres_zapory/capture/<nazwa>/
```

Na przykład:

```
https://192.168.1.1/capture/inside-traffic/
```

Przesyłanie wyników przechwytywania

Zgromadzone w buforze wyniki przechwytywania są przez firewall PIX zapisywane w formacie PCAP. Zapisane pliki mogą być pobrane z zapory, po czym wyświetlone w oprogramowaniu zewnętrznym, takim jak np. Ethereal czy tcpdump. Wyniki można pobierać albo za pomocą protokołu HTTPS, albo wysyłać na serwer TFTP. Aby pobrać dany plik PCAP za pomocą klienta HTTPS, należy wprowadzić adres URL o postaci:

```
https://adres_zapory/capture/<nazwa>/pcap
```

Na przykład:

```
https://192.168.1.1/capture/inside/pcap
```

Wyniki przechwytywania można również przesłać na serwer TFTP — należy skorzystać z polecenia `copy`, w tym przypadku będzie ono mieć następującą postać:

```
copy capture:<nazwa> tftp://<ścieżka>/<nazwa_pliku> [pcap]
```

Jeśli słowo kluczowe `pcap` nie zostanie wprowadzone, to wyniki zostaną przesłane w postaci pliku ASCII. Po wprowadzeniu `pcap` na serwer zostanie przesłany plik w formacie PCAP. Na przykład:

```
PIX1# copy capture:inside-traffic tftp://192.168.99.99/pix-capture pcap
Copying Capture to tftp://192.168.99.99/pix-capture:
```

W powyższym przykładzie zapisane w formacie PCAP wyniki przechwytywania o nazwie `inside-traffic` zostaną przesłane na serwer TFTP o adresie `192.168.99.99` i zapisane w pliku o nazwie `pix-capture`. Po skopiowaniu pliku dane można zanalizować, np. za pomocą wcześniej wspomnianych aplikacji.

Wsparcie techniczne

Firewall PIX może stanowić urządzenie, które pełni w danej sieci rolę o znaczeniu strategicznym. Planowanie architektury sieci wymaga rozważenia różnych możliwości wsparcia technicznego, które będzie w stanie zapewnić obsługę firewalle w sytuacjach awaryjnych. Kwestie tę oczywiście można rozważać jako formę prewencji. Problemy z zaporą można rozwiązywać samemu, można skorzystać z usług firm zewnętrznych (np. dostawcy sprzętu czy oprogramowania) albo ze wsparcia technicznego firmy Cisco. Rozpatrzmy wszystkie trzy możliwości:

- W rozwiązaniu „zrób to sam” wystarczy zakupić odpowiedni sprzęt i oprogramowanie. Poza normalnie dostarczonymi gwarancjami i wsparciem technicznym nie są oferowane żadne usługi dodatkowe. W przypadku awarii jest się skazanym na własną wiedzę i dostępne zasoby.
- W przypadku wsparcia technicznego ze strony firmy zewnętrznej pomiędzy obiema stronami podpisana jest odpowiednia umowa, gwarantująca, że w przypadku awarii sprzętu bądź oprogramowania firma ta zadba o usunięcie usterki w określonym czasie. Choć określona firma może nie dysponować tak dogłębną znajomością problematyki jak firma Cisco, to jako sprzedawca sprzętu może zaoferować znaczny upust na świadczone usługi.
- Wykorzystanie wsparcia technicznego firmy Cisco, tzw. programu SMARTnet, daje pewność, że w każdej chwili ma się dostęp do szerokiej rzeszy ekspertów i najświeższych informacji dotyczących konfiguracji, rozwiązywania problemów i usuwania błędów w oprogramowaniu. Witryna WWW firmy Cisco daje możliwość czerpania z całego bogactwa narzędzi i informacji pomocnych podczas rozwiązywania problemów. Można również skorzystać z członkostwa w CCO (ang. *Cisco Connection Online*) — daje to jeszcze większe możliwości wykorzystania wsparcia technicznego, jak np. możliwość przeglądania opisów zdarzeń w centrum pomocy technicznej Cisco (ang. *Cisco TAC*). Program SMARTnet obejmuje również możliwość wymiany sprzętu i uaktualniania oprogramowania.

Awaria firewalle PIX może dotyczyć dwu rzeczy: oprogramowania lub sprzętu. Aby uchronić się przed uszkodzeniami sprzętu, można kupić sprzęt zapasowy. W zależności od proporcji pomiędzy liczbą urządzeń wykorzystywanych a liczbą urządzeń zapasowych

rozwiązanie to jest mniej lub bardziej opłacalne. Oprogramowanie może zawierać błędy, które zostaną wykryte dopiero po dokonaniu poprawnej konfiguracji. Niektóre funkcje albo polecenia mogą nie działać tak, jak się tego oczekuje, albo mogą nawet nie działać wcale. W każdym przypadku należy wymagać od firmy Cisco informacji, które pozwolą na rozwiązanie problemu, albo nowszej wersji oprogramowania, które nie zawiera określonych błędów. Wykorzystanie programu SMARTnet jest rozwiązaniem dość dobrym — zawsze ma się dostęp do najnowszych wersji oprogramowania. Samodzielna eliminacja błędów w oprogramowaniu jest trudniejsza od eliminowania usterek sprzętu — tu dane urządzenie wystarczy wymienić na nowe. Naniesienie poprawek w kodzie oprogramowania jest bardzo trudne, podjęcie próby obejścia danego błędu często stanowi tylko i wyłącznie stratę czasu.

Monitorowanie i rozwiązywanie problemów z wydajnością

Już wcześniej wspominaliśmy o tym, jakie znaczenie ma odpowiednie dobranie modelu PIX-a do istniejących potrzeb. Prócz natężenia ruchu należy tu rozważyć jeszcze kilka innych czynników. Obciążenie, jaki każdy model PIX-a jest w stanie obsłużyć, tak przy braku szyfrowania, jak i przy wykorzystaniu szyfrowania — przedstawiono w tabeli 11.3. Przed wdrożeniem PIX-a należy się upewnić, że wybrany model sprosta wymaganiom.

Tabela 11.3. Wydajność poszczególnych modeli firewalla PIX

| Model | Maksymalna konfiguracja sprzętowa (CPU, RAM, flash) | Wydajność przy braku szyfrowania | Wydajność przy szyfrowaniu DES | Wydajność przy szyfrowaniu 3DES | Maksymalna liczba równocześnie obsługiwanych tuneli VPN |
|----------|---|----------------------------------|--------------------------------|---|---|
| PIX 501 | AMD SC520 133 Mhz, 16 MB, 8 MB | 10 Mb/s | 6 Mb/s | 3 Mb/s | 5 hostów |
| PIX 506E | Intel Celeron 300 MHz, 32 MB, 8 MB | 20 Mb/s | 20 Mb/s | 16 Mb/s | 25 hostów |
| PIX 515E | Intel Celeron 433 MHz, 64 MB, 16 MB | 188 Mb/s | 33 – 120 Mb/s | 63 Mb/s (l. nieograniczona) 22 Mb/s (l. ograniczona) | 2000 |
| PIX 525 | Intel Pentium III 600 MHz, 256 MB, 16 MB | 360 Mb/s | 120 – 140 Mb/s | 70 Mb/s | 2000 |
| PIX 535 | Intel Pentium III 1 GHz, 1 GB PC 133, 16 MB | 1 Gb/s | 200 Mb/s | 100 Mb/s | 2000 |

Moduł FSWM 1.1 dla przełączników Cisco z serii Catalyst 6500 stanowi urządzenie o wysokiej wydajności, o przepustowości rzędu 5 Gb/s dla ruchu zagregowanego. Nie oferuje ono obsługi tuneli VPN opartych na IPsec.

O całkowitej wydajności firewalle PIX decyduje wydajność trzech komponentów: procesora, pamięci i interfejsów sieciowych. Zasadniczą kwestią jest to, czy obciążenie poszczególnych komponentów mieści się w granicach normy. Aby móc monitorować obciążenia poszczególnych komponentów, należy poznać odpowiednie metody — przedstawiamy je poniżej.

Monitorowanie wydajności procesora

Na procesorze PIX-a ciąży ostateczna odpowiedzialność za realizację wszystkich funkcji firewalle, przekazywanie ruchu, tworzenie tuneli VPN, realizację szyfrowania itd. Jako regułę można przyjąć, że podczas normalnego funkcjonowania obciążenie procesora powinno wynosić około 30 procent. W godzinach szczytowego natężenia ruchu albo np. podczas ataku sieciowego można zauważyć, iż obciążenie procesora wzrasta — jest to normalne. Jednakże jeśli użycie procesora przy normalnym ruchu sieciowym stale utrzymuje się na poziomie powyżej 30 procent, to świadczy to o jego przeciążeniu — należy rozważyć zakup modelu, który będzie oferował większą wydajność.

Różne funkcje obciążają procesor zapory w różnym stopniu, najwięcej czasu procesora zabierają operacje związane z szyfrowaniem (DES i 3DES). Tak więc jeśli zapora obsługuje dużą liczbę tuneli VPN, to należy regularnie monitorować obciążenie procesora. Jeśli obciążenie przekracza dopuszczalne limity, należy rozważyć wyposażenie zapory w kartę VAC (ang. *VPN Accelerator Card*), która odciąży procesor od operacji związanych z obsługą tuneli VPN. Jako rozwiązanie alternatywne można rozważyć też przeniesienie ruchu VPN na dedykowany koncentrator VPN (np. VPN 300 firmy Cisco). Czynnikiem obciążającym procesor jest oczywiście również i normalny ruch sieciowy. Tu również — jeśli natężenie ruchu jest duże, należy regularnie monitorować obciążenie procesora i obserwować wartości szczytowe. Obciążenie procesora najwygodniej monitorować poprzez SNMP, za pomocą takich narzędzi jak MRTG albo HP OpenView.

Na stopień użycia procesora ma również wpływ wykorzystanie poleceń debug. W celu zaoszczędzenia cykli procesora poziom rejestrowanych szczegółów powinien być ustawiony na wymagane w danych okolicznościach minimum. Wszystkie dostępne poziomy rejestrowania przedstawiono w tabeli 11.4. Jeśli istnieje konieczność wykorzystania wyższych poziomów rejestrowania, to należy rozważyć wyłączenie niepotrzebnych komunikatów — służy do tego polecenie `no logging message`.

Tabela 11.4. Poziomy rejestrowania

| Opis | Wartość liczbowa |
|---------------|------------------|
| Emergency | 0 |
| Alert | 1 |
| Critical | 2 |
| Error | 3 |
| Warning | 4 |
| Notification | 5 |
| Informational | 6 |
| Debugging | 7 |

Bieżące opcje i poziom rejestrowania można określić, wprowadzając polecenie `show logging`. Oto przykład ilustrujący działanie polecenia `show logging`, jeśli na zaporze rejestrowanie jest całkowicie wyłączone:

```
PIX1# show logging
Syslog logging: disabled
  Facility: 20
  Timestamp logging: disabled
  Standby logging: disabled
  Console logging: disabled
  Monitor logging: disabled
  Buffer logging: disabled
  Trap logging: disabled
  History logging: disabled
```

Polecenie `show cpu usage`

Polecenie `show cpu usage` wyświetla bieżącą statystykę obciążenia procesora. Wyświetlone informacje dotyczą ostatnich kilku minut pracy zapory, tak więc nie są użyteczne z punktu widzenia potrzeb analizy obciążenia w dłuższym odcinku czasu. Wyświetlone informacje dają jednakże możliwość natychmiastowego stwierdzenia, czy procesor zapory jest przeciążony. Oto przykład użycia tego polecenia:

```
PIX1# show cpu usage
CPU utilization for 5 seconds = 2%; 1 minute: 1%; 5 minutes: 1%
```

W przypadku spadku wydajności PIX-a polecenie to daje możliwość sprawdzenia, czy źródłem takiej sytuacji jest procesor. Podejrzenia takie można mieć np. w sytuacji, gdy zapora realizuje szyfrowanie IPsec. Ostatecznym dowodem będzie porównanie stopnia obciążenia procesora przy włączonym i wyłączonym szyfrowaniu. Po sprawdzeniu obciążenia procesora przy włączonym szyfrowaniu należy je wyłączyć. Ponowne sprawdzenie obciążenia procesora i porównanie wyników pozwoli na stwierdzenie, czy przyczyną spadku wydajności zapory jest właśnie procesor, którego przeciążają operacje związane z szyfrowaniem. Aby mieć pewność, iż prezentowane wyniki są dokładne, polecenie `show cpu usage` należy wprowadzić kilka razy, w pewnych odstępach czasu.

Polecenie `show processes`

Gdy stopień użycia procesora jest zbyt wysoki, to warto pozyskać nieco dokładniejsze informacje na temat źródła takiego stanu rzeczy — polecenie `show cpu usage` tu nie wystarczy. Informacje związane z każdym procesem, który jest uruchomiony na zaporze, można poznać, wykorzystując polecenie `show processes`. Prezentowany jest stan każdego procesu, zużycie pamięci i procesora. Informacje o procesach gromadzone są od chwili uruchomienia firewalla. Efekt wprowadzenia polecenia `show processes` przedstawiono poniżej. Jak widać, liczba wyświetlanych danych jest dość duża — a jest to tylko fragment listingu pochodzącego z firewalla PIX 501, najsłabszego z PIX-ów. Poszczególne procesy nie będą tu omawiane, przedstawimy tylko znaczenie poszczególnych kolumn listingu. Szczegółowe omówienie polecenia `show processes` można znaleźć pod adresem www.cisco.com/warp/public/110/pix_shproc.html.

PIX1# show processes

| | PC | SP | STATE | Runtime | SBASE | Stack | Process |
|----------|----------|----------|----------|----------|----------|-------------|-----------------|
| Hsi | 800b0e09 | 80759798 | 8052ddd8 | 0 | 80758310 | 3532/4096 | arp_timer |
| Lsi | 800b5271 | 8077c880 | 8052ddd8 | 0 | 8077b908 | 3912/4096 | FragDBG |
| Lwe | 8020685d | 808b8e20 | 80507300 | 0 | 808b6ed8 | 7644/8192 | Logger |
| Hwe | 8020a550 | 808bbe8 | 805075b0 | 0 | 808b9f70 | 8008/8192 | tcp_fast |
| Lsi | 80137edd | 809400f0 | 8052ddd8 | 0 | 8093f168 | 3928/4096 | xlate_clean |
| Lsi | 80256f4d | 8096c430 | 8052ddd8 | 0 | 8096b4a8 | 3900/4096 | route_process |
| Mwe | 800d2671 | 809b19e0 | 8052ddd8 | 0 | 809afa68 | 6940/8192 | Ipsec timer |
| Lwe | 8012ff5a | 809daac8 | 80539908 | 0 | 809d9c50 | 3704/4096 | pix/trace |
| Lwe | 8013016a | 809dbb58 | 80539fd0 | 0 | 809dace0 | 3704/4096 | pix/tconsole |
| Hwe | 800b2dd0 | 809dbe8 | 80753b9c | 0 | 809dbd70 | 7196/8192 | pix/incf1 |
| H* | 80015207 | 7ffffe2c | 8052ddc0 | 200 | 809e1ea0 | 12652/16384 | ci/console |
| Csi | 801299b3 | 809e6e88 | 8052ddd8 | 10 | 809e5f30 | 3440/4096 | update_cpu_usag |
| A | B | C | D | E | F | G | H |

Pierwsza litera pierwszej kolumny określa priorytet procesu. Możliwe są cztery priorytety procesów: krytyczny (C, ang. *critical*), wysoki (H, ang. *high*), średni (M, ang. *medium*) i niski (L, ang. *low*). Kolejne dwie litery oznaczają bieżący stan procesu, możliwe stany procesów zebrano w tabeli 11.5.

Tabela 11.5. Stany procesów PIX-a

| Oznaczenie | Opis |
|------------|--|
| * | Proces jest uruchomiony. |
| E | Proces oczekuje na zajście zdarzenia. |
| S | Proces jest gotowy do uruchomienia — uśpiony. |
| rd | Proces jest gotowy do uruchomienia — zaszły warunki aktywacji. |
| we | Proces czeka na zdarzenie. |
| sa | Proces uśpiony do określonej chwili. |
| si | Proces uśpiony na określony przedział czasu. |
| sp | Proces uśpiony na określony przedział czasu. |
| st | Proces uśpiony do upłynięcia czasu timera. |
| hg | Proces jest zawieszony i nie zostanie uruchomiony ponownie. |
| xx | Proces został zakończony, lecz nie został usunięty. |

Dla danego procesu kolumna PC (B) prezentuje licznik programu (ang. *program counter*), kolumna SP (C) — wskaźnik stosu (ang. *stack pointer*). Kolumna STATE (D) określa adres kolejki wątków danego tego procesu. Kolejka wątków może być współdzielona

między różne procesy. W kolumnie `Runtime` (E) wyświetlany jest czas w milisekundach, na jaki dany proces zajął procesor od chwili uruchomienia tego procesu. W kolumnie `SBASE` (F) jest wyświetlany adres początku stosu procesu (ang. *stack base address*). Kolumna `Stack` (G) przedstawia stosunek wykorzystywanej do zaalokowanej pamięci stosu, obie wartości wyrażane są w bajtach. Procesy, które są wykonywane w nieprawidłowy sposób, mogą zawłaszczać obszary pamięci należące do innych procesów. Ostatnia kolumna, `Process` (H), zawiera nazwę danego procesu.

Polecenie `show processes` daje możliwość sprawdzenia, czy któryś z procesów nie zabiera zbyt wielu cykli procesora. Aby to sprawdzić, należy w odstępie minuty dwukrotnie wprowadzić `show processes`. Od wartości `Runtime`, która zostanie podana po wprowadzeniu drugiego polecenia, należy odjąć wartość wyświetloną po wprowadzeniu pierwszego. Otrzymany rezultat stanowi czas w milisekundach, na jaki dany proces zajął procesor w ciągu tej minuty. Istotne jest, by uwzględnić fakt, iż niektóre procesy są kolejgowane do wykonywania w określonych odstępach czasu, podczas gdy inne aktywizują się dopiero po nadejściu danych do przetworzenia. Wartość `Runtime` jest zwykle największa dla procesu `577 poll`, który odpowiada za monitorowanie stanu interfejsów Ethernet w celu określenia, czy w ich buforach nie znajdują się jakieś dane, które trzeba odebrać.

Polecenie `show perfmon`

Jednym ze szczególnie użytecznych poleceń, przeznaczonych do monitorowania wydajności zapory PIX, jest polecenie `show perfmon`. Wyświetla ono szczegółowe statystyki dotyczące translacji, połączeń, działania analizy na warstwie aplikacji, działania mechanizmu AAA itd. Jest to jedyne polecenie, które prezentuje średnie statystyczne wartości liczby połączeń i translacji. Jak można zauważyć w poniższym listingu, poszczególne wartości pogrupowane są wedle protokołów, daje to pewną możliwość określenia rodzaju ruchu, który obciąża procesor zapory czy pamięć RAM w stopniu najwyższym. Opis wartości wyświetlanych po wprowadzeniu polecenia `show perfmon` jest zawarty w tabeli 11.6.

```
PIX1# show perfmon
PERFMON STATS:   Current   Average
Xlates           0/s      0/s
Connections      0/s      0/s
TCP Conns        0/s      0/s
UDP Conns        0/s      0/s
URL Access       0/s      0/s
URL Server Req   0/s      0/s
TCP Fixup        0/s      0/s
TCP Intercept    0/s      0/s
HTTP Fixup       0/s      0/s
FTP Fixup        0/s      0/s
AAA Authen       0/s      0/s
AAA Author       0/s      0/s
AAA Account      0/s      0/s
```

Podobnie jak w przypadku wszelkich statystyk, informacje wyświetlane po wprowadzeniu polecenia `show perfmon` są bezużyteczne, jeśli nie ma się żadnego punktu odniesienia. Aby określić jakieś wartości standardowe, należy prowadzić regularne monitorowanie stanu firewalla. Po ich ustaleniu, dzięki porównaniu wyników bieżących do wartości stanowiących punkt odniesienia — wszelkie anomalie będą łatwo dostrzegalne.

Tabela 11.6. Znaczenie wartości wyświetlanych po wprowadzeniu polecenia `show perfmon`

| Wartość | Opis |
|----------------|---|
| Xlates | Liczba translacji na sekundę. |
| Connections | Liczba nawiązywanych połączeń na sekundę. |
| TCP Conns | Liczba nawiązywanych połączeń TCP na sekundę. |
| UDP Conns | Liczba nawiązywanych połączeń UDP na sekundę. |
| URL Access | Liczba żądań dostępu do adresów URL na sekundę. |
| URL Server Req | Liczba żądań skierowanych do serwera filtrującego adresy URL na sekundę. |
| TCP Fixup | Liczba przekazywanych pakietów TCP na sekundę. |
| TCP Intercept | Liczba pakietów SYN na sekundę, która przekracza wartość dopuszczalną (limit połączeń na wpół nawiązanych). |
| HTTP Fixup | Liczba komunikatów HTTP na sekundę, które zostały poddane analizie w warstwie aplikacji. |
| FTP Fixup | Liczba komunikatów FTP na sekundę, które zostały poddane analizie w warstwie aplikacji. |
| AAA Authen | Liczba żądań uwierzytelnienia AAA na sekundę. |
| AAA Author | Liczba żądań weryfikacji uprawnień AAA na sekundę. |
| AAA Acount | Liczba żądań uprawnionego dostępu AAA na sekundę. |

Monitorowanie stanu pamięci

Stopień użycia pamięci RAM może być podczas określania wydajności zapory równie ważny, jak stopień użycia procesora. W pamięci flash przechowywany jest obraz systemu operacyjnego PIX-a oraz konfiguracja. Dopóki dane te mieszczą się w pamięci flash, to można uznać, iż pamięć nie odgrywa tu żadnej znaczącej roli.

Pamięć RAM, będąca tematem niniejszej części rozdziału, stanowi przestrzeń roboczą firewalle PIX. Podczas rozruchu zapory obraz systemu operacyjnego jest kopiowany z pamięci flash do pamięci RAM. System jest uruchamiany dopiero po skopiowaniu systemu do pamięci RAM. Pamięć ta jest również wykorzystywana przez wszystkie procesy, tu również umieszczane są bufony przeznaczone do obsługi ruchu sieciowego. Z uwagi na fakt, iż pamięć RAM jest używana w tak wielu różnych kontekstach pracy firewalle, ilość wolnej pamięci RAM ma dla wydajności firewalle znaczenie bardzo istotne. W związku z tym stan pamięci RAM powinien być regularnie monitorowany. Do tego celu można wykorzystać kilka różnych poleceń, przedstawiamy je poniżej. Ponadto, podobnie jak w przypadku użycia procesora — stan pamięci RAM może być w wygodny sposób monitorowany poprzez SNMP, za pomocą narzędzi takich jak MRTG albo HP OpenView.

Polecenie show memory

Polecenie `show memory` daje informacje o ilości zainstalowanej i na bieżąco wykorzystywanej pamięci RAM. Oto przykład użycia tego polecenia:

```
PIX1# show memory
16777216 bytes total, 4517888 bytes free
```

Ilość pamięci, jaką zabiera realizowanie określonych operacji, można sprawdzić w prosty sposób. Najpierw firewall należy uruchomić w bardzo podstawowej konfiguracji, wprowadzić polecenie `show memory` i zanotować otrzymany wynik. Następnie należy uruchomić badaną funkcję. Po ponownym wprowadzeniu `show memory` otrzymany rezultat należy porównać z wcześniejszym. Ilości pamięci, jaką zabierają poszczególne funkcje zapory, może być w ten sposób oszacowana w miarę dokładnie.

Polecenie show xlate

Jednym z procesów, które zabierają pewną ilość pamięci RAM, jest translacja adresów. Każda translacja zabiera około 56 bajtów pamięci. Dysponując tą informacją — po wprowadzeniu polecenia `show xlate` można określić ilość pamięci, jaką zajmują wszystkie translacje adresów. Na przykład:

```
PIX1# show xlate
100 in use, 341 most used
```

Mnożąc wyświetloną liczbę przez 56 bajtów, otrzymujemy łączną ilość pamięci, jaką pochłania realizacja translacji adresów. W powyższym przykładzie liczba wykorzystywanych translacji wynosi 100, znaczy to, że obsługa translacji zabiera około 5600 bajtów pamięci RAM.

Polecenie show conn

Każde realizowane przez firewall połączenie sieciowe również zabiera określoną ilość pamięci RAM. Liczba bajtów, jaką pochłania obsługa danego połączenia, zależy od jego rodzaju. Każde połączenie wymaga utworzenia odpowiednich struktur opisujących to połączenie oraz utrzymania informacji o stanie połączenia, informacje te przechowywane są właśnie w pamięci RAM. W przypadku protokołu UDP pojedyncze połączenie zajmuje 120 bajtów, w przypadku protokołu TCP będzie to 200 bajtów. Oto przykład polecenia `show conn`:

```
PIX1# show conn
100 in use, 100 most used
```

W przytoczonym przykładzie firewall realizuje 100 połączeń — jeśli są to połączenia TCP, to zabierają one 20 KB pamięci RAM. Oczywiście liczba połączeń nacechowana jest pewną zmiennością, tak więc w różnych porach dnia jest różna.

Polecenie show block

Po załadowaniu i uruchomieniu konfiguracji firewall PIX rezerwuje pewną ilość pamięci na potrzeby specjalnej obsługi pewnego rodzaju ruchu. Alokacja tej pamięci zachodzi przed wszystkimi innymi, a pamięć jest rezerwowana w postaci zmiennej liczby bloków

o ustalonym rozmiarze. Liczba poszczególnych bloków jest określona za pomocą pewnych wartości granicznych. Dzięki takiej organizacji pamięć jest w razie potrzeby dostępna bardzo szybko — firewall nie musi poświęcać czasu na szukanie, odzyskiwanie albo przesuwanie danych w pamięci. Liczbę bloków można sprawdzić za pomocą polecenia `show blocks`. Na przykład:

```
PIX1# show blocks
  SIZE  MAX   LOW   CNT
    4   1600  1563  1600
   80   400   386   400
  256   500   143   500
 1550  1700  1102  1315
16384    8     8     8
```

Wyjaśnijmy powyższy listing. Kolumna `SIZE` określa rozmiar bloku w bajtach. Bloki 4-bajtowe są wykorzystywane do obsługi np. DNS, IKE, TFTP — szybkiego ruchu małych ilości danych. Bloki 80-bajtowe używane są do przechowywania komunikatów hello, związanych z obsługą ciągłości dostępu oraz nadmiarowych potwierdzeń TCP. Bloki 256-bajtowe służą do przechowywania komunikatów związanych ze stanem obsługi ciągłości dostępu. 1550-bajtowe bloki wykorzystywane są do przechowywania ramek sieci Ethernet, które przechodzą przez firewall. Bloki 16384-bajtowe wykorzystywane są tylko i wyłącznie do obsługi ruchu Gigabit Ethernet.

Kolumna `MAX` określa maksymalną liczbę bloków danego rodzaju, jaka jest dostępna na firewallu. Kolumna `LOW` określa minimalną liczbę bloków, jaka była dostępna od czasu uruchomienia zapory. Biorąc rzecz matematycznie, odejmując wartość z kolumny `LOW` od wartości z kolumny `MAX` — można obliczyć maksymalną liczbę bloków, które były wykorzystywane od czasu uruchomienia zapory. Kolumna `CNT` określa bieżącą liczbę wolnych bloków pamięci. Aby wyzerować liczniki `LOW` i `CNT` — należy posłużyć się poleceniem `clear blocks`.

Monitorowanie wydajności sieci

Zatłoczone interfejsy sieciowe mogą obniżyć ogólną wydajność firewalla. Należy mieć pewność, iż interfejsy zapory są w stanie obsłużyć ruch, który jest na nie kierowany. Stan interfejsów sprawdzić można za pomocą kilku różnych poleceń PIX-a.

Polecenie `show interface`

Jednym z tych poleceń jest polecenie `show interface`. Daje ono możliwość sprawdzenia zużycia pasma oraz szerokiej gamy liczników różnych błędów. Polecenie to było już omawiane we wcześniejszej części rozdziału, tak więc przedstawionych informacji w tym miejscu powtarzać nie będziemy.

Polecenie `show traffic`

Analizę stanu obciążenia interfejsów można ograniczyć do określenia liczby i łącznego rozmiaru pakietów przechodzących przez poszczególne interfejsy — informacje te prezentowane są po wprowadzeniu polecenia `show interface`. Sposób ten jest jednak o tyle niewygodny, że polecenie `show interface` trzeba wprowadzić dla każdego z interfejsów osobno.

Polecenie `show traffic` daje informację przekrojową, wyświetla statystyki dotyczące liczby i łącznego rozmiaru pakietów, które przeszły przez każdy z interfejsów. Jak można zauważyć w poniższym listingu, polecenie `show traffic` daje również informacje o przedziale czasu, w którym były gromadzone informacje statystyczne. Czas ten jest liczony od chwili uruchomienia zapory albo od chwili wyzerowania liczników za pomocą polecenia `clear traffic`. Dla wszystkich interfejsów statystyki ruchu napływającego i wychodzącego liczone są osobno:

```
PIX1# show traffic
outside:
  received (in 10035.150 secs):
    2 packets      678 bytes
    0 pkts/sec     0 bytes/sec
  transmitted (in 10035.150 sees):
    14 packets     1026 bytes
    0 pkts/sec     0 bytes/sec
inside:
  received (in 10035.150 secs):
    0 packets      0 bytes
    0 pkts/sec     0 bytes/sec
  transmitted (in 10035.150 secs):
    15 packets     900 bytes
    0 pkts/sec     0 bytes/sec
```

Wydajność firewalla PIX a protokół ident

Jeden z protokołów ma w kontekście wydajności chronionej PIX-em sieci znaczenie szczególne. Mowa tu o protokole `ident` (ang. *identification protocol*), który jest określony w dokumencie RFC1413. Protokół ten służy do identyfikacji klientów przy wykorzystaniu protokołu TCP i dotyczy takich usług, jak np. HTTP, FTP czy POP. Gdy dany klient łączy się z serwerem, np. POP, który wykorzystuje protokół `ident` — serwer ten w celu identyfikacji klienta nawiązuje połączenie z jego 113. portem TCP i pobiera pewne dane, które identyfikują użytkownika. Teoretycznie protokół `ident` zapobiega nawiązaniu połączeń z nieokreślonych źródeł (co wykorzystywane jest np. przez spamatorów) — wymaga realizacji połączeń ze źródeł, które potrafią udzielić informacji o użytkowniku. W praktyce protokół `ident` może być w prosty sposób ominięty.

Domyślnie na firewallu PIX obsługa protokołu `ident` jest wyłączona — za jego pomocą informacje o użytkowniku sieci wewnętrznej mogłyby przeniknąć do sieci publicznej, z punktu widzenia bezpieczeństwa sieci prywatnej jest to niedopuszczalne. Ubocznym skutkiem zablokowania obsługi protokołu `ident` mogą być obserwowane przez użytkowników sieci wewnętrznej znaczne opóźnienia w odpowiedziach serwerów, które próbują dokonać identyfikacji. W skrajnym przypadku serwery mogą nie odpowiadać wcale.

W celu identyfikacji problemów z protokołem `ident` poziom rejestrowania PIX-a należy ustawić na debugowanie i obserwować, czy zaporą odrzuca próby połączeń z 113. portem TCP. Jeśli sytuacja taka ma miejsce — problem należy rozwiązać na jeden z trzech sposobów:

1. Można skontaktować się z administratorem serwera, na którym jest uruchomiana obsługa protokołu `ident` i poprosić o jej wyłączenie. Oczywiście będzie to konieczne w przypadku każdego serwera, który sprawia problem.

2. Można zdecydować się na przepuszczanie ruchu związanego z protokołem ident, w tym celu należy posłużyć się listami dostępu albo ścieżkami. Należy jednak pamiętać, iż działanie takie może naruszać bezpieczeństwo sieci — informacje o sieci prywatnej mogą przeciekać na zewnątrz.
3. Można posłużyć się poleceniem `service resetinbound`. Jest to rozwiązanie zalecane. Po wprowadzeniu polecenia `service resetinbound` firewall będzie wysyłać do żądającego identyfikacji serwera pakiet TCP RST (ang. *reset*), co jest przez serwer interpretowane jako brak obsługi protokołu ident. Po otrzymaniu takiego komunikatu serwer przyjmuje normalny tryb pracy i odpowiada na żądania klienta bez potrzeby identyfikacji i żadnych dodatkowych opóźnień. Opisane zachowanie PIX-a po wprowadzeniu polecenia `service resetinbound` dotyczy wyłącznie ruchu, który jest blokowany. PIX informuje o zablokowaniu ruchu, zamiast po cichu go odrzucać.

Podsumowanie

W tym rozdziale przedstawiono metodologię rozwiązywania problemów, która bazuje na modelu OSI. W takim ujęciu rozwiązywanie problemów rozpoczyna się od warstw niższych i stopniowo bada aspekty odpowiadające coraz wyższym warstwom modelu OSI. Postępowanie takie ma tę zaletę, iż pozwala na eliminację błędów począwszy od najprostszych, a skończywszy na najbardziej złożonych. Dzięki temu zawsze istnieje pewność, że prostsze funkcje, od których zależą funkcje właśnie badane, są już zweryfikowane.

Wiedza to potęga. Znajomość różnic w poszczególnych modelach PIX-a jest podczas rozwiązywania problemów szczególnie istotna. Niektóre modele PIX-a, takie jak np. PIX 501 czy PIX 506, nie oferują obsługi ciągłości dostępu. Znajomość tego typu detali może ochronić przed stratą czasu na uruchamianie funkcji, które nie są obsługiwane przez dany model zapory. Inne informacje, które warto znać, to liczba równocześnie obsługiwanych połączeń oraz liczba i rodzaj obsługiwanych interfejsów sieciowych (np. Ethernet, Token Ring).

Choć firewall PIX obsługuje tylko ograniczoną liczbę rodzajów sieci, to jednakże znajomość wykorzystywanego w tych sieciach okablowania często decyduje o powodzeniu procesu, który ma na celu usunięcie awarii. W przypadku sieci Ethernet firewall PIX wykorzystuje złącza RJ45, jako schemat podłączania złączy firma Cisco zaleca standard TA586A/B, w przypadku sieci Gigabit Ethernet wykorzystywane są złącza duplex-SC przeznaczone dla światłowodów wielomodowych. Kabel „failover” stanowi przykład rozwiązania wykorzystywanego wyłącznie przez firmę Cisco, choć opartego na standardowych złączach.

Aby firewall PIX mógł pełnić właściwe sobie funkcje, musi mieć łączność z odpowiednimi sieciami oraz możliwość trasowania pakietów do określonych hostów. Do tego celu wykorzystywane są trasy statyczne oraz protokół RIP. Zagadnienia administracji PIX-em obejmują zatem również i kwestie związane z rozwiązywaniem problemów z osiągalnością sieci i hostów IP.

W przypadku PIX-a do przekazywania pakietów pomiędzy sieciami konieczna jest translacja adresów. Wśród poleceń, które można wykorzystać do powstających tu problemów, są takie jak: `show xlate`, `show nat`, `show global`. Należy pamiętać, by po każdym kroku związanym z rozwiązywaniem problemów, jak również po każdej konfiguracji PIX-a — wprowadzać polecenie `clear xlate`.

Kolejną kwestią, z którą można się spotkać podczas rozwiązywania problemów z komunikacją, jest kwestia dostępu. Należy mieć pewność, że dostęp do sieci prywatnej mają tylko i wyłącznie określone hosty sieci zewnętrznej. Do weryfikacji dostępu wykorzystuje się polecenia takie jak: `show conduit`, `show access-list` i `show access-group`.

Obsługa IPsec stanowi bodajże najbardziej skomplikowaną w konfiguracji funkcję firewalla PIX. Rozwiązywanie problemów z IPsec jest równie skomplikowane. W rozdziale tym zostały omówione tylko podstawowe polecenia, umożliwiające weryfikację możliwości IPsec. Podczas rozwiązywania problemów z IPsec należy najpierw zadbać o funkcję ISAKMP, następnie należy się zająć samym IPsec. Choć IPsec zależy od ISAKMP, to jednak zależność taka w drugą stronę już nie zachodzi.

Wraz z wprowadzeniem wersji oprogramowania 6.2 firewall PIX zyskał bardzo użyteczną funkcję — przechwytywanie i analizę pakietów. Mowa tu o poleceniu `capture`. Przechwycone dane mogą być przeglądane i analizowane zdalnie, nawet w przeglądarce WWW. Rozwiązanie to eliminuje konieczność instalowania w badanych sieciach snifferów pakietów produkowanych przez firmy trzecie.

Najlepszym nawykiem związanym z rozwiązywaniem problemów jest aktywne monitorowanie, które ma na celu wykrywanie problemów, jeszcze zanim doprowadzą do utraty możliwości kontroli nad zachowaniem urządzenia. Działania aktywne mogą w przypadku PIX-a dotyczyć różnych aspektów i polegać np. na gromadzeniu danych związanych z wydajnością procesora, zużyciem pamięci czy statystyk związanych z użyciem pasma sieci.