Firewall 1 NG FP3

25 marzo 2005

Indice

I Management I **6**

1 Introduzione **7**
1.1 Funzionalità Offerte da VPN-1/FW-1 . . . 7
1.1.1 Funzionalità di Filtro . . . 7
1.1.2 Funzionalità di NATting . . . 7
1.1.3 Funzionalità di VPN . . . 7
1.1.3.1 Site to Site . . . 7
1.1.3.2 Host to Site . . . 7
1.1.4 Gestione Centralizzata degli Upgrade . . . 8
1.1.4.1 Licenze . . . 8
1.1.4.2 Prodotti . . . 8
1.1.5 Semplice Intrusion Detection System (Smart Defence) . . . 8
1.1.6 Open Platform for SECurity . . . 8
1.2 Tecnologie di Firewall . . . 8
1.2.1 Vecchia Tecnologia (Packet Filtering) . . . 8
1.2.2 Vecchia Generazione (Application Layer Gateway) . . . 8
1.2.3 Vecchia Generazione (Circuit Layer Gateway) . . . 8
1.2.4 Nuova Generazione (Stateful Inspection) . . . 8
1.3 Architettura NG . . . 9
1.3.1 SMART Client . . . 9
1.3.2 Mangement Server . . . 9
1.3.3 Enforcement Module . . . 9
1.4 Security Virtual Network Foundation (CPShared) . . . 9
1.5 Distribuited Deployment . . . 9

2 RuleBase and Properties Setup **10**
2.1 SMART DashBoard . . . 10
2.1.1 Secure Client - Secure Remote . . . 10
2.1.2 Actualize dello SMART Map . . . 10
2.1.3 Content Vector Protocol Manager . . . 10
2.1.4 Inspection Module Flow . . . 11
2.1.5 Inizializzazione dei FQDN . . . 11
2.1.6 Stateful Inspection . . . 11
2.2 SMART DashBoard Base . . . 11
2.2.1 Definitions . . . 11
2.2.2 Rule base . . . 11
2.2.2.1 Default Rule . . . 11
2.2.2.2 Cleanup (None of the Above) . . . 11
2.2.2.3 Stelth . . . 12
2.2.3 Tipi di Regole . . . 12
2.2.3.1 Esplicite . . . 12
2.2.3.2 Implicite . . . 12

2.2.3.3 Ordine di Lettura delle Regole . . . 12

3 SMART View Tracker 13
3.1 Generazione e Transito Log Record . . . 13
3.2 Tipologie di Visualizzazione . . . 13
3.3 Blocking Connection . . . 14

4 SMART View Status 15

5 Authentication 16
5.1 Authentication Types . . . 16
5.1.1 User Authentication . . . 16
5.1.2 Client Authentication . . . 16
5.1.3 Session Authentication . . . 17
5.1.3.1 Sign On Methods . . . 17
5.2 Authentication Schemas . . . 17
5.2.1 OS/Password . . . 17
5.2.2 VPN-1/FW-1 Password . . . 18
5.2.3 TACACS . . . 18
5.2.4 Radius . . . 18
5.2.5 SecurID . . . 18
5.2.6 S/Key . . . 18

6 Network Address Translation 19

7 Backup 20

8 Upgrades 21

9 License 22

II Mangement II 23

10 Installation 24
10.1 Upgrade . . . 24
10.1.1 Procedura . . . 24
10.1.1.1 Minimizzazione Downtime . . . 25
10.1.2 SMART Update . . . 25
10.1.2.1 Upgrade del Software . . . 25
10.1.2.2 Upgrade Licenze . . . 25
10.2 Installation . . . 25
10.2.1 Operazioni Preliminari . . . 25
10.2.2 Comandi . . . 26
10.2.3 Procedura . . . 26
10.2.3.1 SVN Foundation . . . 26
10.2.3.2 VPN-1/FW-1 Management . . . 26
10.2.3.3 SMART Client . . . 26
10.2.3.4 Policy Server . . . 27
10.3 Disinstallation . . . 27
10.3.0.5 Comandi di Disinstallazione . . . 27
10.3.0.6 Ordine di Disinstallazione . . . 27

11 Tracking and Alert **28**
11.1 Definizioni . . . 28
11.1.1 Funzionamento . . . 28
11.2 Tracking Commands . . . 29
11.2.1 Definizione dei Comandi di Alert . . . 29
11.2.2 Comandi di Log . . . 29
11.3 Default Tracking . . . 29
11.3.1 Log Time Setting . . . 30

12 Load Balancing **31**
12.1 SYN Defender . . . 31
12.1.1 Parametri . . . 31
12.2 Load Balancing . . . 31
12.2.1 Load Balancing Algorithm . . . 32
12.2.2 Configuration Properties . . . 32
12.2.2.1 Server Availability . . . 32
12.2.2.2 Persistency . . . 32
12.2.2.3 Server Load Measurement . . . 32
12.2.3 Logical Server Type . . . 32
12.2.3.1 HTTP Logical Server . . . 33
12.2.3.2 Other Logical Server . . . 33

13 Voice Over IP Traffic **34**
13.1 Generalità . . . 34
13.1.1 Protocolli Supportati . . . 34
13.1.2 Quality Control . . . 34
13.1.2.1 Bandwith . . . 34
13.1.2.2 Voice Quality . . . 34
13.1.2.3 Security . . . 34
13.1.3 H.323 . . . 35
13.1.4 SIP . . . 35

14 Content Security **36**
14.1 Risorse . . . 36
14.1.1 URI Resource . . . 36
14.1.1.1 Match . . . 36
14.1.1.2 Action . . . 36
14.1.1.3 CVP . . . 37
14.1.2 FTP Resource . . . 37
14.1.2.1 Match . . . 37
14.1.2.2 Action . . . 37
14.1.2.3 CVP . . . 37
14.1.3 SMTP Resource . . . 37
14.1.3.1 Match . . . 37
14.1.3.2 Action1 . . . 37
14.1.3.3 Action2 . . . 37
14.1.3.4 CVP . . . 37
14.1.4 Common Internet File System . . . 37
14.1.5 TCP Resource . . . 37
14.1.5.1 General . . . 37
14.1.5.2 CVP o UFP . . . 37
14.2 Security Servers . . . 37
14.2.1 FTP Security Server . . . 38
14.2.2 SMTP Security Server . . . 38

14.2.2.1 Security Sendmail . . . 38
14.2.2.2 SMTP Addres Translator . . . 38
14.2.3 HTTP Security Server . . . 38
14.3 URL Filtering Protocol . . . 38
14.4 Content Vectoring Protocol . . . 38
14.4.1 Load Sharing and Chaining . . . 38

15 Cryptography and VPNs **40**

16 Certificate Authority **41**

17 Virtual Private Network Setup **42**
17.1 Tecniche Impiegate . . . 42
17.1.1 Packet Tunneling . . . 42
17.1.2 Crittografia . . . 42
17.2 IPSEC . . . 43
17.2.1 Authentication Header . . . 43
17.2.2 Encapsulation Security Payload . . . 43
17.2.3 Internet SEcurity Association and Key Management Protocol . . . 43
17.2.3.1 Security Association . . . 43
17.2.3.2 Key Management Protocol . . . 43
17.2.3.3 Internet Key Exchange . . . 43
17.2.3.4 Fasi . . . 43
17.3 Struttura Pacchetto . . . 44
17.3.1 Struttura Pacchetto TCP Standard . . . 44
17.3.2 Struttura Semplificata Pacchetto IPSEC . . . 44
17.4 Configurazione . . . 44

18 SecuRemote **45**

19 Secure Client **46**

III Extras **47**

20 Domande Frequenti **48**
20.1 Domande Frequenti CCSA . . . 48
20.1.1 Modulo 1 (VPN-1/FW-1 Overview) . . . 48
20.1.2 Modulo 2 e 3 (Smart DashBoard) . . . 49
20.1.3 Modulo 4 (Smart View Tracker, Smart View Status) . . . 49
20.1.4 Modulo 5 (Authentication) . . . 50
20.2 Domande Frequenti CCSE . . . 51
20.2.1 Modulo 3 (Load Balancing) . . . 51
20.2.2 Modulo 4 (VoIP) . . . 52
20.2.3 Modulo 5 (Content Security) . . . 52
20.2.4 Modulo 6 Cryptography and VPN . . . 52

21 SNMP **53**
21.1 Entities . . . 53
21.1.1 Managed Nodes . . . 53
21.1.2 Management Station . . . 54
21.1.3 Management Information . . . 54
21.1.4 Management Protocol . . . 54
21.2 Management Information Structure . . . 55
21.2.1 Abstract Syntax Notattion 1 . . . 55

21.2.1.1 Standard Object Definition Language 55
21.2.2 Data Description Language 55
21.2.2.1 Types 55
21.2.2.2 Object Identifier 55
21.2.3 ASN Transfer Syntax 55
21.2.3.1 Basic Encoding Rules 56
21.3 Protocol 56

22 VPN-1/FW-1 Useful Line Commands **57**

23 VPN-1/FW-1 Default Communication TCP/IP Ports **58**

Parte I

Management I

Capitolo 1

Introduzione

1.1 Funzionalità Offerte da VPN-1/FW-1

1.1.1 Funzionalità di Filtro

Packet Filtering: filtro del traffico in transito attraverso il firewall sulla base delle proprietà indirizzo/porta sorgente/destinazione, tenendo conto dello stato di ogni connessione (Tabelle di stato)

Application Gateway: semplice funzionalità di filtro, a livello applicativo, per un numero ridotto di protocolli (e.g. HTTP, SMTP)

URL Filtering Protocol:

Content Vectoring Protocol:

1.1.2 Funzionalità di NATting

1.1.3 Funzionalità di VPN

Fornita attraverso IPSEC/IKE

1.1.3.1 Site to Site

Verso reti esterne (servizi VPN all'altro capo, protocolli standard)

1.1.3.2 Host to Site

Verso singoli elaboratori (SecuRemote, Secure Client)

1.1.4 Gestione Centralizzata degli Upgrade

1.1.4.1 Licenze

1.1.4.2 Prodotti

1.1.5 Semplice Intrusion Detection System (Smart Defence)

1.1.6 Open Platform for SECurity

1.2 Tecnologie di Firewall

1.2.1 Vecchia Tecnologia (Packet Filtering)

- application independent
- Layer III (nessun tipo di controllo a livello superiore)
- Scalable
- Fast

Vengono aperte tutte le porte "efemerals" (dalla 1024 alla 5000), per permettere ai client di colloquiare con Internet.

1.2.2 Vecchia Generazione (Application Layer Gateway)

Detti anche Proxy Applicativi, ovvero Proxy che si interpongono, a livello applicativo (dunque ISO-OSI 7) fra il client ed il server, entrando nel merito del contenuto dei pacchetti. Devono saper fare da client e da server per ogni particolare tipo di applicazione supportata.

- buon livello di sicurezza
- computazionalmente pesante
- limitata compatibilità a livello applicativo
- interrompe la connessione client-server (doppio numero di socket)

1.2.3 Vecchia Generazione (Circuit Layer Gateway)

Detti anche Proxy a Circuito, ovvero Proxy che si interpongono, a livello di Connessione (ISO_OSI 4,5)

1.2.4 Nuova Generazione (Stateful Inspection)

Lo Stateful Inspection è stato introdotto nel 1995 ca.

- tra Layer II e Layer III
- Dynamic State Tables (tabelle di stato, mantengono le informazioni relative ad ogni singola connessione)
- connessione a moduli esterni (CVP)
- apre solo le porte realmente utilizate dal client
- Communication Derived State
- Application Derived State (Content Vector Protocol, URL Filtering Protocol)

- Information Manipolation (funzioni aritmetiche e logiche per il QoS: FloodGate)

Tutti i firewall hanno adottato la Tabella di Stato. Quante più informazioni sono sulla tabella, tanto più può fare il firewall.

1.3 Architettura NG

1.3.1 SMART Client

SMART= Security Management ARchiTecture

SMART DashBoard Policy Editor

SMART View Tracker Log Viewer

SMART View Status System Status

SMART Update demone di update automatico (non viene stoppato in seguito allo stop del firewall da script)

SMART View Monitor

1.3.2 Mangement Server

1.3.3 Enforcement Module

1.4 Security Virtual Network Foundation (CPShared)

FrameWork di base dei componenti Check Point. Comprende i seguenti componenti:

Security Internal Communications Canale crittografico tra Enforcement Module e Management Server basato su TLS. La Certification Authority viene istallata sul Mangement Server. Tutti i moduli e le Management hanno un proprio certificato tramite il quale si authenticano.

CP Registry

CP Shared demone CPShared

cpconfig programma di configurazione a livello testuale

License Utilities

SNMP Daemon

1.5 Distribuited Deployment

- Licenza (Local, Central)
- Prodotto (e.g. SMART Update[1])

[1] Hot FIx 1 per FP3 si istalla su Modulo e Management. La GUI va disinstallata e reinstallata la nuova. Gravi bachi sulla VPN di FP3.

Capitolo 2

RuleBase and Properties Setup

2.1 SMART DashBoard

1. Frame a Sinistra
   (a) Object Tree
2. Frame a Destra
   (a) Policy Editor Tabs
      i. Security Policy Editor Tab
      ii. Network Address Translation Policy Editor Tab
      iii. VPN Manager Policy Editor Tab
      iv. QoS Policy Editor Tab (FloodGate)
      v. DeskTop Security Policy Editor Tab
      vi. Web Access Policy Editor Tab
   (b) Objects List
   (c) Smart Map

2.1.1 Secure Client - Secure Remote

Softwares per la connesione diretta in VPN tra client e Firewall Check Point. Inserisce un Inspect Engine tra il driver della scheda di rete ed il driver NDIS (TCP/IP).

Secure Client rispetto a Secure Remote ha in più:

- Personal Firewall
- Controllo delle Regole (locali)
- a pagamento

2.1.2 Actualize dello SMART Map

Serve per riconoscere tutte le reti che possono essetre create, inserendole nella object list. In questo modo si possono correggere errori (dovuti magari a digitazione errata). E' possibile stampare la configurazione della rete.

2.1.3 Content Vector Protocol Manager

Può essere istallato su una macchina a parte, diversamente da quanto accdeva con FW1 4.x. Non si capisce come mai non venga citato come prodotto a parte.

2.1.4 Inspection Module Flow

- Spoofing fatto allo stesso livello di FW1 4.x
- NATting
- Routing

2.1.5 Inizializzazione dei FQDN

- Creazione dell'oggetto
- Apertura delle porte 18181 e 18182 da parte del firewall
- Initialize (bottone)

Per la connessione con i client i certificati non sono obbligatori. La prima volta che si istallano le GUI avviene il fingerprint (HASH functions).

2.1.6 Stateful Inspection

- Architettura (no Tecnologia!)
- Track, Analize, Act on:
  - Connection Status
  - Packet Header
  - Fragmentation
  - informazioni contenute
- Riassemblamento dei Pacchetti

2.2 SMART DashBoard Base

2.2.1 Definitions

Spoofing capacità di cambiarel'header dei pacchetti, in modo da falsare l'indirizzo del sorgente o destinatario. Si può obbligare la macchina che risponde a passare per un certo percorso.

Not Defined no regole antispoofing

Network Defined sulla base dei calcoli che lui fa

Specific scegliendo la network specifica (problemi di NAT). Può utilizzarsi anche con host singoli

2.2.2 Rule base

2.2.2.1 Default Rule

Regola che viene inserita di default ogni volta che si richiede di inserire una nuova regola:

SRC	DST	IFVIA	Proto	Action	Track	Target	
Any	Any	Any	Any	Drop	None	Policy Target	Any

2.2.2.2 Cleanup (None of the Above)

Regola che viene utilizzata se nessuna delle precedenti matcha (per questo ha il secondo nome NotA). Dovrebbe essere sempre inserita come ultima regola.

SRC	DST	IFVIA	Proto	Action	Track	Target	
Any	Any	Any	Any	Drop	Log	Policy Target	Any

2.2.2.3 Stelth

Regola che nasconde il Firewall. Dovrebbe essere inserita tra le prime, subito dopo le regole esplicite che servono per accedere al firewall (in modo diverso dall'accesso tramite SMART GUI, che viene settato con cpconfig ed a cui corrispondono delle regole implicite, ovvero impostate automaticamente dal firewall):

SRC	DST	IFVIA	Proto	Action	Track	Target	
Any	<FW-module>	Any	Any	Drop	Log	Policy Target	Any

2.2.3 Tipi di Regole

2.2.3.1 Esplicite

2.2.3.2 Implicite

Regole inserite automaticamente dalla Management a seconda delle scelte effettuate nelle Global Properties:

- non sono visibili per defualt
- hanno un colore diverso (per rimarcare la non modificabilità diretta)

Si dividono in:

- First
- Before Last
- Last

2.2.3.3 Ordine di Lettura delle Regole

1. IP Spoofing
2. NAT
3. Implicit First
4. Administrator (User)
5. Implicit Before Last
6. Administrator (Last Rule)
7. Last

Capitolo 3

SMART View Tracker

GUI tramite la quale è possibile visualizzare i tracciamenti relativi alle regole o gli oggetti per i quali sia stato impostato esplicitamente la creazione di log.

3.1 Generazione e Transito Log Record

Tutti i pacchetti che transitano attraverso il firewall, passano per il kernel side.

- fwd esegue il merge dei frammenti di una stessa connessione in un log record
- fwd assegna al log record un LUUID (Log Unification Unique IDentifier), aggiugendo un numero identificativo, data e ora
- fwd trasferisce il log record nel log database (<Management-Server:$FWDIR/log/fw.log)
- Lo Unification Engine invia il log record al fwm in tempo reale, quando sono richiesti da uno Smart View Client.

Se dovesse venire meno la comunicazione tra Enforcement Module e Management Server, fwd bufferizza i log localmente. I log dovrebbero essere inviati verso la management in modo accorpato (non singolarmente uno per uno).

3.2 Tipologie di Visualizzazione

Log Mode: modalità di viasualizzazione in cui sono mostrate tutte le informazioni disponibili relative a eventi verificatisi nel passato, relative ad eventi di sicurezza.Diversamente dalle precedenti versioni di FW-1, non è possibile, in fase di definizione di un insieme di oggetti e regole, indicare la quantità di informazioni da tracciare. Vengono tracciato tutto ciò che è possibile. Viceversa in fase di visionamento dei log è possibile selezionare i campi da visualizzare o utilizzare le 12 "viste" di default dello SMART View Tracker

Audit Mode: modalità di visualizzazione in cui sono mostrati gli eventi relativi a operazioni di manutenzione dei componenti Check Point. I seguenti campi sono mostrati:

Number: numero sequenziale

Date: data di rilevamento

Time: tempo di rilevamento

Application: applicazione cui si è acceduto

Operation: operazione effettuata

Category: categoria di appartenenza della operazione

Name: nome assegnato

Administrator: nome di login dell'amministratore che ha eseguito la operazione

Client: postazione di lavoro dalla quale ci si è collegati

Info: informazioni addizionali

Active Mode: modalità di visualizzazione in cui sono mostrate le seguenti informazioni relative alle connessioni correntemente attive:

Elapsed: durata della connessione

Bytes: numero di bytes trasferiti

Start Date: momento in cui la connessione ha avuto inizio

Connection ID: identificativo della connessione

3.3 Blocking Connection

Nello Smart View Tracker in modalità di visualizzazione "Active Mode" è possibile bloccare determinate connessioni (che risultino pericolose). Dal menù Tools → Block Intruder:

- Block from this Source
- Block to this Destination
- Block on this Ports

Rispetto alle versioni precedenti non c'è il blocco in base al numero di ID del log record.

Capitolo 4

SMART View Status

Capitolo 5

Authentication

5.1 Authentication Types

Vi sono tre tipi di autenticazione:

- User
- Client
- Session

Ognuna di questa autenticazioni necessita dell'inserimento di username e password. Nel caso di mancata autenticazione (utente o password sbagliata) l'account non viene bloccato, nel caso lo schema di autenticazione utilizzato sia uno dei tre interni a VPN-1/FW-1; nel caso di schemi estermi (e.g. TACACS, Radius) dipende da come sono settati questi ultimi.

5.1.1 User Authentication

Si tratta del tipo di autenticazione più sicura. Si viene autenticati per ogni nuova sessione (appare un pop-up a video). Il firewall esegue Natting e Proxying, sui seguenti protocolli:

- ftp
- http
- rlogin
- telnet

5.1.2 Client Authentication

Si tratta della connessione meno sicura dele tre, ma la più utilizzata in genere. Si viene autenticati tramite indirizzo IP. Non prevede l'attività di proxying.

- SIGNON:
  - http://<ip-enforcement-module>:900 (seguire link a video)
  - telnet <ip-enforcement-module> 259 (scegliere opzione 1)
- utilizzo della connettività
- SIGNOFF

- http://<ip-enforcement-modul>:900 (seguire link a video)
- telnet <ip-enforcement-module> 259 (scegliere opzione 2)

Anche a seguito dello spegnimento della macchina si rimane collegati. Gli unici due modi per eseguire il SIGNOFF sono:

- SIGNOFF esplicito dal client (metodi visti pocanzi)
- Time-out
- Reistallazione delle Policy sul Modulo (reset di tutte le autenticazioni)

Per via delle connessioni di SIGNON che devono avvenire in modo esplicito verso l'Enforcement Module, la regola di autenticazione client va inserita prima della Stelth Rule.

5.1.3 Session Authentication

E' la autenticazione di livello di sicurezza intermedio fra le due precedentemente viste. Analogamente alla Client non viene effettuato il Proxying delle connessioni e dunque è valida per ogni servizio. Richiede la istallazione di un agente che sta nel CD di Check Point. E' possibile configurare l'agente in modo da variare i parametri di durata della autenticazione (che viene effettuata tramite pop-up, analogamente alla User Authentication).

La procedura di Session Authentication avviene secondo i seguenti steps:

Connection: l'agente fa una richiesta di connessione al modulo

Session Authentication Agent: il modulo richiede all'agente le informazioni necessarie all'istaurazione della sessione (e.g. utente e password)

Client ID & Password: l'agente invia le informazioni al modulo

Session Authentication: la connessione viene istaurata (se tutto è andato a buon fine)

5.1.3.1 Sign On Methods

Manual: telnet, http

Partially Automatic: SIGNON tramite pop-up sul client, SIGNOFF anche tramite spegnimento della macchina

Fully Automatic: Comportamento iniziale da User, successivamente da Session

Agent Automatic Sign On: contatta in automatico l'agente, ma non per ogni sessione, solo "una tantum" (comportamento simile alla Session Authentication)

Single Sign On: si usa per controllare l'accesso a server esterni. Controlla se può lavorare <utente>@<macchina>

5.2 Authentication Schemas

5.2.1 OS/Password

Si utilizzazno le password del S.O. (le utenze vanno inserite u aper una "a mano").

- utenza nel S.O. del modulo
- l'account deve appartenere ad un "Windows Authentication Domain"

5.2.2 VPN-1/FW-1 Password

Molto conveniente, poichè anche se non si ha la utenza nel S.O. funziona (DB sulla management)

5.2.3 TACACS

5.2.4 Radius

5.2.5 SecurID

5.2.6 S/Key

Basato su nome e numero (⇒Hash Functions)

Capitolo 6

Network Address Translation

La grossa novità rispeto alle versioni precedenti è che ora il posizionamento temporale delle operazioni di NATting e Routing può essere modificato. In particolare è possibile fare in modo da eseguire prima il NATting rispetto al routing (che è di solito il settaggio di default). In questo modo non è più necessario:

- inserire le route statiche
- inserire le entry fisse nella tabella arp (che poi di solito avevano difficoltà ad essere pubblicate, almeno su Sun)

Capitolo 7

Backup

Capitolo 8

Upgrades

Capitolo 9

License

Parte II

Mangement II

Capitolo 10

Installation

10.1 Upgrade

Controllare le Policy per vedere se le regole possono essere usate su NG, attraverso i comandi:

fw checkobj: controlla che la definizione degli oggetti sia compatibile con l'upgrade

fw cpmi_upgrade: esegue il controllo onde poter effettuare l'upgrade della Management

- se si ha Solaris 2.6:
  - eseguire l'upgrade a 4.1 SP4
  - reboot
  - upgrade a Solaris 8
  - reboot
  - upgrade da 4.1 a NG
  - reboot

10.1.1 Procedura

- upgrade la Management, lasciando la compatibilità con 4.1
- upgrade gli SMART Client
- upgrade degli Enforcement Module
- cambiare la definizione degli oggetti che descrivono i moduli nelle policy

Quando si esegue l'upgrade i seguenti componenti sono trasferiti, con cambiamenti, automaticamente alla nuova versione (e nella directory della versione corrente):

- database (FWauthDB)
- Key View DB
- RuleBase
- Properties
- Encryption Parameters

10.1.1.1 Minimizzazione Downtime

Per minimizzare il downtime (dovuto all'enforcement module in stato di upgrade, o alla Management, dunque inattivi) creare una macchina speculare aggiornata e sostituirla alla originale

10.1.2 SMART Update

10.1.2.1 Upgrade del Software

Tramite tale componente è possibile upgradare, su tutti i componenti cui siano state istallate le hot fix:

- SVN Foundation
- VPN-1/FW-1
- FloodGate
- Secure Client Policy Server
- SMART View Monitor
- OPSEC

Al termine reinstallare le policy sugli Enforcement Module, poichè durante lupgrade essi perdono il loro stato.

10.1.2.2 Upgrade Licenze

Se devo rifare un nodo:

- tolgo la licenza dal nodo
- reinstallo
- rimetto la licenza (locale o centralizzata)

10.2 Installation

10.2.1 Operazioni Preliminari

I requisiti minimi di sistema sono:

- 40 MB di spazio su disco
- 128 MB di RAM

Inoltre è necessario:

1. Assicurarsi che i parametri di rete siano correttamente configurati, in particolare il Routing
2. Assicurarsi che ogni macchina sulle varie reti raggiunga le altre
3. Abilitare il Forwarding
4. Eseguire una Hardenizzazione della macchina (e.g. disabilitare il NetBEUI su Windows, inetd su Unix)

10.2.2 Comandi

I comandi da utilizzare per istallare i componenti Check Point sono forniti nel CD stesso del prodotto. Nel prosieguo, per semplicità, verrà indicato con "." la directory ove viene montato il CD sui sistemi Unix.

Windows: inserire il CD ed eseguire l'autorun
ATTENZIONE: su Windows 2000 l'IP Forwarding deve essere abilitato esplicitamente agendo sui file di registro, mediante regedit

Solaris: montare il CD ed eseguire ./UnixInstallScript.

ATTENZIONE: a partire dalla versione NG FP1 lo script è fatto male: prima di eseguire la istallazione copia il contenuto del CD nella directory /cp_tmp (che cancella e crea durante la esecuzione dello script solaris2/install_pkg, onde non è possibile usare un soft link verso un'altra locazione del FIle System). Accertarsi preliminarmente di avere circa 400 MB di spazio nella /; se così non fosse, copiare il contenuto del CD su una directory sufficientemente capiente in modo da poter modificare la definizione di CP_TMP in ./solaris2/install_pkg.

Linux: montare il CD ed eseguire ./UnixInstallScript. Si appoggia direttamente al supporto rpm di sistema. Il programma di istallazione ./wrappers/unix/Install_Linux e comunque i componenti della suite di CP richiedono le librerie di compatibilità con le vecchie versioni delle libc++. Nel caso non siano presenti sul sistema è possibile istallare la versione che si trova nel CD di Check Point:

1. # cp ./linux /libcpc++-libc6.1.2.so.3 /usr/lib
2. # ldconfig

Nokia IPSO:

10.2.3 Procedura

Qualora si voglia stallare più di un componente su una macchina seguire la sequenza di sotto proposta.

10.2.3.1 SVN Foundation

Si tratta delle librerie e dei binari di base. Non vengono presentate opzioni durante la istallazione. Deve essere presente su ogni macchina che rechi software Check Point.

10.2.3.2 VPN-1/FW-1 Management

tipologia: chiede se la Management deve essere:

- primary: ovvero di tipo master
- secondary: entra in funzione qualora la master non sia in funzione

Backward Compatibility: scegliere se abilitare o meno la possibilità di amministrare moduli di versioni precedenti

Installation Path: permette di modificare il path di istallazione predefinito

10.2.3.3 SMART Client

Chiede quali elementi istallare. Di default li mette tutti.

10.2.3.4 Policy Server

Enforcement Module. Non vengono presentate opzioni

10.3 Disinstallation

10.3.0.5 Comandi di Disinstallazione

I comandi per disinstallare i componenti Check Point su una macchina sono quelli forniti dal Sistema Operativo:

Windows: aprire la finestra "Install/Disinstall Application"

Solaris: comandi pkgrm.

1. Verificare i componenti istallati:
   #pkginfo -p | grep CP
2. Disintallare i componenti, secondo quanto desunto dal comando precedente:
   # pkgrm <pkg-name>

Red Hat Linux: comandi RPM

1. Verificare i componenti istallati:
   # rpm -qa | grep CP
2. Disinstallare i componenti secondo quanto desunto dal comando precedente:
   # rpm -e <pkg-name>

Nokia IPSO: IPSO è praticamente un Free BSD 3.5.1

10.3.0.6 Ordine di Disinstallazione

La disinstallazione dei componenti Check Point va eseguita secondo un certo ordine. In ogni tipo di server CP l'ultimo componente che va eliminato è "CP SVN Foundation", dal momento che crea l'ambiente CP di base.

Nel caso particolare di un server Stand Alone i componenti vanno disinstallati secondo l'ordine:

1. SMART Clients
2. Enforcement Module
3. Management Server
4. SVN Foundation

Capitolo 11

Tracking and Alert

11.1 Definizioni

Tracking: processo di definizione dei parametri sulla base dei quali effettuare Log o Alert.

La definizione del tracking avviene mediante:

- valorizzazione della colonna "Track" nella RuleBase
- opportuni check nella creazione degli oggetti

Le opzioni del Tracking determinano la generazione di:

- niente
- voci di Log
- voci di Log e attivazione di trigger

Il tracking quindi scaturisce due tipi di azione:

logging: conserva le informazioni complete relative ad un evento, creando un archivio storico

alerting: comando real-time customizzabile

11.1.1 Funzionamento

Il tracciamento segue il seguente percorso:

1. L'Enforcement Module rileva la necessità di generare un tracciamento sulla base degli eventi che stanno accadendo e della politica istallata. Comunica le informazioni di Tracking ai Log Server di competenza
2. I Log Server (su cui è eseguito il processo alertd), generalmente la Management stessa, recepisce le informazioni e, sulla base delle regole istallate, determina il tipo di azione (log o alert)
3. Le informazioni di tracciamento viaggiano verso la destinazione opportuna nelle forme e nei modi stabiliti dalla configurazione

Per quanto detto i comandi relativi al'alerting devono essere istallati sulla Management (o Log Server) e precisamente nella directory
$FWDIR/bin

In tale directory è presente il comando di alert di default [fw]alert, che corrisponde ad un Pop-Up Alert sulla Workstation di Management

11.2 Tracking Commands

Nella definizione delle regole e degli oggetti è possibile utilizzare uno dei nove comandi di Tracking (3 di Log e 6 di Alert)

11.2.1 Definizione dei Comandi di Alert

I comandi che possono essere usati nella definizione delle Rule Base e degli oggetti, possono essere, almeno in parte, configurati in base alle proprie esigenze.

Allo scopo, aprire il Tab: Global Properties$\Longrightarrow$Log and Alert $\Longrightarrow$Alert Commands. In tale Tab è possibile configurare gli alert configurabili, ovvero:

Mail: invio di Alert Tramite e-mail

SNMP: invio di Alert tramite SNMP Trap (l'SNMP deve essere istallato sul S.O. del Log Server)

User Defined 1: (per default $FWDIR/bin/alert)

User Defined 2: (per default $FWDIR/bin/alert)

User Defined 3: (per default $FWDIR/bin/alert)

Il Pop-Up Alert Script non è dato modificarlo.

Inoltre è possibile settare, per tutti gli alert la possibilità di inviare l'Alert corrispondente verso lo SMART View Status.

11.2.2 Comandi di Log

I comandi di Log non sono configurabili e corrispondono ai 3 seguenti predefiniti:

None: non effettua alcun tipo di tracciamento

Log: invia tutti i dati possibile in modo da inserirli nello storico

Account: invia le sole informazioni necessarie alla determinazione del consumo

11.3 Default Tracking

Nel seguente paragrafo vengono presentati gli eventi per i quali è possibile configurare le opzioni di tracking di default, indicando uno dei 9 comandi da usare. Allo scopo andare sul Tab Global Properties $\Longrightarrow$Log and Alert:

VPN successful key exchange:

VPN packet handling error: errori relativi a AH o ESP

VPN configuration & key exchange error: errori relativi a violazione dei domini di encryption o problemi durante una delle due fasi IKE

IP Option drop: pacchetto con opzioni IP (droppato)

Administration notification: messaggi all'amministratore riguardanti eventi, operazioni da eseguire, etc.

SLA violation:

Connection matched by SAM: connessione bloccata dal "Suspicious Activity Monitoring"

Dynamic object resolution failure:

Inoltre nello stesso Tab è possibile abilitare, tramite check button, il log di ogni autenticazione avvenuta su HTTP.

11.3.1 Log Time Setting

Sempre nel Tab Global Properties $\Longrightarrow$Log and Alert è possibile configurare gli intervalli di tempo relativi ai log ed in particolare:

Excessive log grace period:

SmartView Tracker resolving:

VirtualLink statistic logging interval: frequenza delle statistiche di SLA

Status fetching interval: frequenza di interrogazione da parte della Management verso i client

Capitolo 12

Load Balancing

12.1 SYN Defender

Come si intuisce dal nome, questo componente cerca di difendere i server dagli attacchi di SYN Flooding, che mirano a riempirne la coda di backlog.

Il meccanismo è semplice: il firewall controlla ogni sequenza di istaurazione della connessione client-server TCP (SYN, SYN/ACK, ACK) mediante un timer, per default settato a 10 secondi; allo scadere del tempo fa in modo da resettare la connessione. Esistono tre modalità di funzionamento, elencate per invasività crescente:

passive gateway: invia il SYN al server e il SYN/ACK al client. Qualora non dovesse arrivare l'ACK manda un FIN al server. In questo modo si intacca la coda di backlog del server, in modo limitato nel tempo

gateway: invia il SYN al server, il SYN/ACK al client e un ACK generato in vece del client al server. Qualora non dovesse arrivare l'ACK vero (quello del client) invia un FIN al server. In questo modo non viene intaccata la coda di backlog del server ma viene istaurata una connessione magari non necessaria

relay: risponde come se fosse un proxy, rispondendo in vece del server. Non invia il SYN al server. Invia tutta la sequenza la server, solo dopo aver ricevuto l'ACK dl client. In questo caso non vengono intaccate minimamente le risorse del server, gravando unicamente sul firewall. Introdotto con FP2

12.1.1 Parametri

E' posibile settare i seguenti parametri relativi al comportamente di SYN Defender:

Maximum Sessions: agisce sul baklog del firewall

Time Out: secondi di attesa dell'ACK dal client

Sebbene siano parametri di nodo (da settare nelle proprietà dell'Enforcement Module) sono configurabili anche nelle Global Properties per compatibilità con le versioni precedenti.

12.2 Load Balancing

Componente che mette in Load Balancing un insieme di macchine che erogano uno stesso servizio, permettendo di condividere e distribuire il carico di lavoro. Funziona creando un Server virtuale sul Firewall, munito di un unico indirizzo IP, che redireziona il client verso uno dei server disponibili, mediante un opportuno algoritmo.

Per utilizzare questa feature occorre aver istallato Connect Control, la cui licenza costa circa la metà rispetto alla istallazione di Hardware apposto per il Load Balancing (e.g. Arrow Point).

12.2.1 Load Balancing Algorithm

Determina quale dei server è opportuno che prenda in carico la nuova richiesta di comunicazione. Check Point implementa i seguenti algoritmi di selezione:

Random: calcolo pseudo casuale

Round Robin: a turno

Round Trip: secondo il tempo di risposta ai 3 ECHO Request inviate

Domain: secondo il nome del dominio, in modo che sia il più vicino possibile al client. Utilizzabile esclusivamente con HTTP server

Server Load: sulla base delle informazioni di carico (CPU, Memoria, Applicativo) fornite dal Load Measuring Agent appositamnte istallato sul server, comunicante sulla porta 18212

12.2.2 Configuration Properties

Da Global Properties $\Longrightarrow$Connect Control è possibile configurare i seguenti parametri, accorpati secondo area di appartenenza

12.2.2.1 Server Availability

Verifica della disponibilità di un server

Server availability check interval: intervallo di tempo trascorso il quale l'Enforcement Module cercherà di determinare la disponibilità di un server

Server check retries: numero di volte consecutive in cui il server può non rispondere prima di considerare il server non disponibile

12.2.2.2 Persistency

Meccanismo analogo al Keepalive

Persistent server timeout: intervallo di tempo durante il quale le richieste di connessione sono inviate allo stesso server

12.2.2.3 Server Load Measurement

Load agents port: porta attraverso la quale comunica il Load Measuring Agent

Load neasurement interval: intervallo di tempo tra una misura di carico e l'altra

12.2.3 Logical Server Type

In dipendenza dal livello ISO-OSI su cui viene effettuato il redirezionamento, si ha la necessità di definire due tipi di Logical Server differenti

12.2.3.1 HTTP Logical Server

In questo tipo di load balancing il redirezionamento viene effettuato al livello più alto, ovvero l'applicazione. Il funzionamento è il seguente:

1. L'Enforcement Module rileva la richiesta HTTP e la inoltra al Load Balancing, che calcola il server effettivo verso cui occorre proseguire la comunicazione
2. L'Enforcement Module notifica al client, tramite HTML, il redirezionamento sul server HTTP fisico
3. Il resto della comunicazione avviene tra client e server fisico

Le regole di NATting relative sono create automaticamente all'atto della definizione del server logico.

Occorre invece creare le seguenti 2 regole esplicite:

Source	Destination	Port	Action
Any	Logical Server	HTTP	Allow
Any	Physical Server Group	HTTP	Allow

12.2.3.2 Other Logical Server

In questo tipo di load balancing il redirezionamento viene effettuato al livelli 3, ovvero network, a tutto vantaggio della efficenza, tramite l'ausilio delle tabelle ARP, mediante aggiunta di una voce transitoria nella tabella. Il funzionamento è il seguente:

1. L'Enforcement Module rileva la richiesta non-HTTP e la inoltra al Load Balancing, che calcola il server effettivo verso cui occorre proseguire la comunicazione
2. L'Enforcement Module inserisce la voce di Reverse Hide NAT (Logical Server $\longrightarrow$Physical Server) nella tabella di ARP
3. Il resto della comunicazione avviene modificando gli indirizzi del server all'interno dei pacchetti

Capitolo 13

Voice Over IP Traffic

Le tecnologie Voice over IP permettono di veicolare il traffico telefonico per mezzo dei canali di comunicazione dati consentendo di effettuare un notevole risparmio, per via della trasmissione in forma numerica, specie per le chiamate a lungo chilometraggio. Per questa ragione queste tecnologie vengono sempre più adottate, non solo dalle singole società ma anche dai gestori di rete stessa (vedi Telecom Italia).

13.1 Generalità

Ovviamente i due interlocutori telefonici devono avere accesso alla stessa LAN o WAN, per far in modo che esista un camminamento da un apparecchio all'altro.

13.1.1 Protocolli Supportati

Check Point Firewall-1 supporta i seguenti protocolli di comunicazione VoIP:

- H.323
- SIP

13.1.2 Quality Control

Quando viene configurato il supporto VoIP per un ambiente enterprise, occorre porre attenzione ai seguenti aspetti:

13.1.2.1 Bandwith

Le comunicazioni telefoniche richiedono un feeedback immediato tra i due interlocutori, onde è necessario che i pacchetti VoIP abbiano la precedenza sugli altri e comunque sia riservato ad essi una certa porzione di banda qualora la rete sia vicina alla soglia di saturazione

13.1.2.2 Voice Quality

In dipendenza da vari fattori, quali:

Latency: tempo di attesa dato dall'attraversamento della rete

Compression: compressione dei campioni di voce sui canali vocali

13.1.2.3 Security

In Italia, in via delle leggi vigenti, non è concesso criptare una connessione telefonica

13.1.3 H.323

13.1.4 SIP

Capitolo 14

Content Security

Content Security estende le capacità di data inspection ai livelli 5, 6, 7 della pila ISO-OSI, mediante componenti interne al kenel di Firewall-1 o tramite il supporto di applicazioni esterne, che comunicano mediante le librerie OPSEC. Il meccanismo di attivazione è affidato alla definizione e utilizzo di Resources nella regole.

14.1 Risorse

Come detto in precedenza, il controlo dei contenuti viene attivato mediante il rinvenimento di una regola che specifica non soltanto il protocollo da utilizzare ma anche una risorsa.

Le risorse si definiscono tramite il Tab relativo alle risorse. Per tutte è possibile settare un server CVP che effettui un'ulteriore analisi; per evitare il click nervoso degli utenti, è possibile contestualmente settare il flag "Reply Order" che invia subito al client un pacchetto contenente nulla per simulare l'arrivo della risorsa, che intanto viene analizzata dal CVP.

14.1.1 URI Resource

Rappresenta una risorsa, generalmente HTTP.

14.1.1.1 Match

Schema: HTTP, FTP, Gopher

Methods: GET, POST e PUT

Host: nome dell'host

Path: percorso della risorsa

Query: contenuto della URL successivo al "?"

14.1.1.2 Action

Redirection

Strip java code

Strip ActiveX Tag

Strip Javascript tag

14.1.1.3 CVP

Eventuale Server CVP.

14.1.2 FTP Resource

Rappresenta un file che transita mediante FTP.

14.1.2.1 Match

Methods: PUT o GET

filename: restrizioni sulla base del nome del file (accetta semplici espressioni regolari)

14.1.2.2 Action

14.1.2.3 CVP

14.1.3 SMTP Resource

Rappresenta una e-mail.

14.1.3.1 Match

From field

To field

header

attachment type: analisi della classificazione MIME

attachment size: per inibire l'invio di e-mail onerose

14.1.3.2 Action1

14.1.3.3 Action2

14.1.3.4 CVP

14.1.4 Common Internet File System

Rappresenta uno share di tipo SMB (NetBIOS).

14.1.5 TCP Resource

14.1.5.1 General

14.1.5.2 CVP o UFP

14.2 Security Servers

I Security Server sono generalmente coinvolti qualora occorrano le seguenti due evenienze:

Client Auth: mediante definizione opportuna della azione da eseguire in una determinata regola

Risorsa Particolare: mediante definizione opportuna del protocollo (Add with Resource) in una determinata regola

I Security Server forniscono queste due funzioni fondamentali come nella tabella seguente:

Server	Authentication	Content Security
TELNET	yes	no
RLOGIN	yes	no
FTP	yes	yes
HTTP	yes	yes
SMTP	no	yes

concordemente con le caratteristiche dei protocolli:

Authentication: se il protocollo prevede nativamente la autenticazione

Content Security: se il protocollo prevede scambio di risorse e non flussi generici di informazioni o comandi

I Security Server che analizzeremo in questo capitolo sono quelli che forniscono funzionalità di Content Security, eventualmente rafforzabile mediante adozione di un CVP esterno.

14.2.1 FTP Security Server

La funzione di Content Security è affidata ai criteri:

14.2.2 SMTP Security Server

La funzione di Content Security è affidata ai criteri di Match:

14.2.2.1 Security Sendmail

Applicazione che effettua l'SMTP Relay, prevenendo attacchi di connessione diretta verso il server SMTP aziendale.

14.2.2.2 SMTP Addres Translator

Fornisce la funzionalità di cambiare l'indirizzo del mittente, in modo da nascondere la vera identità, riproponendo il nome vero nella e-mail di risposta.

14.2.3 HTTP Security Server

14.3 URL Filtering Protocol

Protocollo proprietario Check Point, mediante il quale vengono scambiate le informazioni relative alle URL da filtrare. La porta utilizzata è la 18182.

Firewall-1 riesce a gestire fino a 50 URL da filtrare. Successivamente è necessario dotarsi di un URL filtering esterno in modo che:

- non ci sia sovraccarico di lavoro per il firewall
- sia più facile manutenere l'insieme delle URL definite

14.4 Content Vectoring Protocol

14.4.1 Load Sharing and Chaining

Il CVP Manager può essere istallato su un Enforcement Module separato. Gestisce le macchine in:

Load Sharing: suddivisione del lavoro fra CVP server che effettuano lo stesso tipo di controllo

Chaining: creazione di una "pipe" tra i server CVP che devono effettuare un controllo in sequenza

Capitolo 15

Cryptography and VPNs

Privacy: solo il destinatario può leggere il messaggio

Authenticity: stabilisce l'identità del mittente

Integrity: stabilisce la correttezza del messaggio

Capitolo 16

Certificate Authority

Capitolo 17

Virtual Private Network Setup

Insieme di tecniche per creare una canale sicuro di interconnessione tra 2 entità (tipicamente 2 reti) utilizzando Internet come mezzo di trasporto.
Le tecnologie utilizzate sono:

IP SECurity: protocollo di incapsulamento dei frame IP dentro altri frame, previa criptazione

Crypto IP Encapsulation: protocollo di incapsulamento a livello Network (vedi http://www.cipe.org)

Tunnel SSL: incapsulamento effettuato a livello applicazione, di ogni singola applicazione, tramite SSL

Point to Point Tunneling Protocol: protocollo definito dalla Microsoft (RFC 2637) per la creazione di tunnel sicuri, nelle comunicazioni End to End. SSupportato anche su altre piattaforme (vedi http://www.poptop.org)

Layer 2 Data Protocol: detto anche Layer 2 Firewall, protocollo proprietario CISCO che effettua la incapusulazione del TCP/IP direttamente dal livello Data Link

Una buona implementazione di una Virtual Private Network deve garantire:

1. Secrecy: segretezza della comunicazione, mediante criptazione dei pacchetti
2. Integrity: integrità del messaggio, mediante Message Digest (Hash) dei pacchetti
3. Authenticity: verifica dell'autenticità del mittente, mediante Digital Signature

17.1 Tecniche Impiegate

Per garantire i tre punti cui sopra occorre dunque utilizzare delle tecniche adeguate:

17.1.1 Packet Tunneling

Incapsulamento di un pacchetto (originato da uno dei due end point della connessione) all'interno di un altro, destinato a viaggiare sulla rete non sicura, tipicamente IP dentro IP. In questo modo si crea una rete virtuale in quanto ad ogni end point pervengono pacchetti con indirizzi interni.

17.1.2 Crittografia

Per rendere la rete virtuale anche privata occorre garantire i requisiti di sicurezza, onde poichè si transita su un canale non sicuro, è necessario l'utilizzo dell crittografia ed in particolare:

- algoritmi simmetrici: per la criptazione dei messaggi

- algortimi di hash: per la veritifica di integrità dei messaggi
- algoritmi asimmetrici: usati in unione con i message digest per la firma dei messaggi

17.2 IPSEC

Estensione del Protocollo IP per la realizzazione di VPN. Si compone di vari protocolli al suo interno.

17.2.1 Authentication Header

Definito nell'RFC 2402, permette l'autenticazione del pacchetto tramite "Strong Encryption" dell'header IP.

Per default comunica sulla porta 51 TCP.

17.2.2 Encapsulation Security Payload

Definito nell'RFC 2406, permette la realizzazione dei meccanismi di secrecy ed integrity del contenuto del pacchetto, mediante:

- cifratura del contenuto, tramite DES, 3DES o analogo
- firma del risultato mediante hash (MD5, SHA1)

Per default comunica sulla porta 50 TCP.

17.2.3 Internet SEcurity Association and Key Management Protocol

Definito nella RFC 2408, permette, attraverso i suoi componenti (IP SEcurity Services) di:

- autenticare un "communication peer"
- effettuare il management dei meccanismi e parametri di sicurezza
- generare le chiavi
- effettuare la "mitigation" (DoS, Reply Attack)

Per default comunica sulla porta 500 UDP.

17.2.3.1 Security Association

Stabilisce in modo dinamico i meccanismi (algoritmi, tecniche) ed i parametri (chiavi, lunghezze) utilizzati per garantire la sicurezza.

17.2.3.2 Key Management Protocol

Protocollo di amministrazione della generazione delle chiavi pubbliche e private.

17.2.3.3 Internet Key Exchange

Detto anche ISAKMP/Oakley, garantisce lo scambio delle chiavi.

17.2.3.4 Fasi

Esistono, quindi, 2 fasi di funzionamento di una VPN mediante IPSEC:

Fase 1: IKE

Fase 2: AH, ESP

17.3 Struttura Pacchetto

17.3.1 Struttura Pacchetto TCP Standard

20 bytes IP Header	20 bytes TCP Header	Payload

17.3.2 Struttura Semplificata Pacchetto IPSEC

20 bytes IP Header	AH	ESP

Per quanto detto, IPSEC si "sostituisce" al TCP standard onde deve essere, in generale, compilato insieme al kernel per poter funzionare.

17.4 Configurazione

E' possibile configurare diverse connessioni, diversi tunnel. Per ognuno di essi deve essere noto almeno:

nome: nome che identifica la connessione

left machine: macchine da cui parte la connessione

ip: IP pubblico della macchina

FQDN: Nome dominio completamente specificato

subnet: rete di appartenenza (che deve essere posta in tunnel)

nexthop: indirizzo del Gateway

RSASigKey: chiave pubblica della macchina (per l'AH)

right machine: ma su cui termina la connessione

auth by: metodo di signature (RSA, DSA, etc.)

Capitolo 18

SecuRemote

Capitolo 19

Secure Client

Parte III

Extras

Capitolo 20

Domande Frequenti

20.1 Domande Frequenti CCSA

Nel manuale ci sono le informazioni che vertono sull'85% delle domande. Il resto va studiato tramite l'uso del prodotto. La maggior parte delle domande verte su:

- autenticazione
- NAT
- analisi delle regole

Nel rispondere alle domande vanno tenuti presenti alcune proprietà generalmente valide:

"Ce l'ho tutte": le certificazioni generalmente hanno lo scopo di mostrare le caratteristiche peculiari di uno o più prodotti ma anche quello di convincere della migliore qualità di questi rispetto a quanto proposto dalla concorrenza. Per questo motivo spesso le domande sono formulate in modo che la risposta evidenzi come non ci siano cose che VPN-1/FW-1 non sia in grado di espletare. Nel dubbio, quindi, conviene dare le risposte che mostrino

"E' più facile": da sempre, effettivamente, Check Point ha posto l'accento, nella fase di sviluppo dei suoi prodotti, alla facilità d'uso rispetto ai prodotti alternativi. Spesso le domande sono poste in modo da evideziare gli automatismi di configurazione esistenti. Nel dubbio, quindi, conviene fornire le risposte che evidenzino la semplicità d'uso di tale prodotto.

20.1.1 Modulo 1 (VPN-1/FW-1 Overview)

1. Quali sono le Tab visibili la prima volta che apre lo SMART DashBoard?
   - Security Policy Editor Tab
   - Object Tree
   - Smart Map
   - Object List
2. Differenza SIC-FQDN?
   (a) Sono praticamente la stessa cosa: il certificato istallato lega indissolubilmente al FQDN (Fully Qualified Distinguish Name). Qualora si dovesse cambiare nome: cpconfig per rigenerare il certificato.
3. Dove va posizionato il firewall? Tra la Intranet ed il mondo esterno

4. Quello da cui il firewall non può proteggere:
   (a) attacco interno
   (b) ciò che non passa dal firewall
5. Cosa controlla lo Stateful Inspection?
   (a) tutti i pacchetti in entrata e tutti i pacchetti in uscita
6. Perchè lo Staful Inspection è più sicuro del PF e Proxy?
   (a) perchè l'analisi viene fatta anche a livello 4-7

20.1.2 Modulo 2 e 3 (Smart DashBoard)

1. Fin quando una regola appena disabilitata è valida?
   (a) finchè non viene eseguito l'install delle policy
2. Da quando una regola nascosta è attiva?
   (a) da subito [solo che non è visibile, serve per il colpo d'occhio]
3. Da menù Rules è possibile fare l'unhide di tutte le regole?
   (a) sì: Rules→Hide →Unhide All
4. Quali sono i meccanismi per "Improve Module"?
   (a) regole più matchate all'inizio [di modo che scorra meno regole possibili]
   (b) mettere le macchine più accedute nel file hosts. (Unix: /etc/hosts, WinNT: %WINDIR%\system32\driver\
   (c) [Policy →Global Properties →Log and Alert →
      i. Excessive Log Grace Time
      ii. Smart View Tracker Resolving

   ]
5. Requisiti di sistema?
   (a) 40 MB spazio su disco
   (b) 128 MB RAM
   (c) [non vengono più richieste le Service Pack minime di sistema richieste]

20.1.3 Modulo 4 (Smart View Tracker, Smart View Status)

1. Se la connessione tra Enforcement Module e Management Server termina di funzionare, vengono perduti i log records?
   (a) no! vengono salvati localmente sul modulo finchè non si ripristina la connessione
2. E' possibile trattare i log con prodotti di terze parti?
   (a) si! Tramite OPSEC e le librerie:
      i. LEA (Log Export API)
      ii. ELA (Event Logging API)

[Il prodotto deve essere agganciato tramite CVP]

3. Quali sono le modalità di visualizzazione dei log?

   (a) Log Mode [log delle regole con Track == log]
   (b) Active Mode [log delle connessioni attive]
   (c) Audit Mode [log dei cambiamenti di configurazione del FW]

4. Come fare per vedere per una particolare connessione da quanto tempo è attiva, quanti byte sono passati, il tempo totale, etc?

   (a) Utilizzare l'Active Mode

5. Cosa si può fare dal menù File dello Smart View Tracker?

   (a) Open
   (b) Open New Window
   (c) Save As [salva il filtro di visualizzazione corrente]
   (d) Export [esporta il file correntemente visualizzato localmente, in modalità testo]
   (e) Switch Active File [stessa cosa di fw logswitch sulla Management]
   (f) Purge Active File [cancella il contenuto del file corrente sulla Management]

6. Quanti Log [file di log] si possono vedere dallo Smart View Tracker [in contemporanea]?

   (a) un file alla volta

7. Quante sono le finestre dello Smart View Status?

   (a) Modules View
   (b) Details View
   (c) Sstem Alert

8. Icone da ricordare:

   (a) Untrusted (comunicazione, ma non trust: problemi di certificato, magari combiato FQDN)
   (b) No Response (non risponde: è morto?)
   (c) Attention (non c'è problema di comunicazione, ma bisogna dare una controllata. e.g. uninstall delle policy)

20.1.4 Modulo 5 (Authentication)

1. Quali sono i tipi di autenticazione?

   (a) User
   (b) Client
   (c) Session

2. Perchè eseguendo la Client Authentication tramite connessione http all'inidirizzo del modulo sulla porta 259, non si viene autenticati?

   (a) perchè la 259 è la porta per la autenticazione tramite telnet e non http.

3. Quali sono i servizi supportati dalla User Authentication?
   (a) ftp
   (b) http
   (c) rlogin
   (d) telnet
4. Cosa succede qualora si cerchi di autenticarsi su un Enforcemente Module sul quale siano asenti regole di autenticazione?
   (a) non si viene autenticati [il messaggio è qullo standard: user or password incorrect]
5. Il tempo di attesa è fisso o variabile?
   (a) qualora si usino schemi di autenticazione che si appoggiano a macchine esterne (e.g. Radius) il tempo di risposta può aumentare
6. L'ordine delle regole viene sempre rispettato?
   (a) Solo nel caso della User Authentication, qualora sia presente una regola meno restrittiva successivamente, si passa per quella (anzichè per la regola di autenticazione)
7. Quanti sono i tentativi di autenticazione?
   (a) 3
8. Quali sono i messaggi a video nel caso di errata autenticazione?
   (a) User: unknown user or bad password
   (b) Client:
   (c) Session:
9. Su quali utenti si riperquote la modifica del Template utente?
   (a) solo sugli utenti definiti successivamente
10. Il Template utente può essere usato come utente?
    (a) no! [ovvio: si tratta solo di un'insieme di scelte di default, comode per clickare sul minor numero di bottoni possibile in fase di definizione delle utenze]

20.2 Domande Frequenti CCSE

20.2.1 Modulo 3 (Load Balancing)

1. Riconoscimento Algortimo di Balancing analizzando le figure
2. POrta di default del Load Measuring Agent
   (a) 18212
3. Quali algoritmi esistono
   (a) Random
   (b) Round Robin

   (c) Domain
   (d) Round Trip
   (e) Server Load

4. Cosa serve aver istallato per utilizzare il Load Balancing

   (a) Connect Control

20.2.2 Modulo 4 (VoIP)

1. Quali sono i protocollo di VoIP supportati da Check Point

   (a) H.323
   (b) SIP

20.2.3 Modulo 5 (Content Security)

1. Che cos'è il Content Security
   estende lo scope di inspection del modulo fino al livello 7
2. Come si fa a fare Content Security senza l'uso di CVP
   per fare Antivirus occorre necessariamente un CVP
3. Settaggio dell'Antivirus

   (a) definire un nodo
   (b) definire il fatto che sul nodo ci sia un CVP (OPSEC Application)
   (c) definire la URI con il CVP associato
   (d) definire la regola contenente la risorsa URI appena creata

20.2.4 Modulo 6 Cryptography and VPN

1. Applicando una chiave simmetrica su un cleartext cosa ottengo
   un ciphertext

Capitolo 21

SNMP

Il Simple Network Managemet Protocol è un metodo sistematico per il controllo e la manutenzione di una rete di computers.

Check Point lo utilizza per varie attività, tra cui il controllo dello stato dei nodi (SMART View Status) e ne riprende spesso la terminologia (i.e. il termine "oggetto" per definire una entità su sui definire regole all'interno dello SMART DashBoard) e la struttura logica ed architeturale (struttura client server).

Dal canto suo l'SNMP si basa notevolmente sui meccanismi di comunicazione CPU-dispositivi, interni agli elaboratori:

- objects$\longleftrightarrow$I/O ports
- SNMP trap $\longleftrightarrow$Interrupt Request ($\longrightarrow$trap)

Dell'SNMP sono stati definite versioni successive. Di seguito sono elencate le più diffuse:

SNMPv1: maggio 1990 (RFC 1157)

SNMPv2: RFC 1441-1452

SNMPv2c

SNMPv2*

SNMPv3:

21.1 Entities

21.1.1 Managed Nodes

Device capaci di:

- comunicare il proprio stato di funzionamento verso il mondo esterno
- ricevere comandi dall'esterno

Per poter eseguire tali funzioni, deve essere presente sul sistema un "management process" ovvero un SNMP Agent.

Ogni agente inoltre mantiene costantemente aggiornate, una serie di informazioni, in un DB locale di variabili che descrivono lo stato attuale e storico del dispositivo.

21.1.2 Management Station

Computer general purpose, contenenti software apposito per l'istruzione degli agenti presenti sui nodi da amministrare, in modo da:

- istruire i comandi
- recepire ed analizzare le informazioni di stato

per ogni nodo.

Tutta la intelligenza, relativa all'SNMP, risiede sulla management, in modo da limitare l'impatto computazionale dell'agente sui nodi.

21.1.3 Management Information

Per essere compatibile con tutte le marche di dispositivi esistenti, è necessario definire, in modo molto preciso, la natura delle informazioni mantenute. Ovvero la Management Station deve isturire l'agente su quali informazioni aggiornare e conservare, in modo da poterle reperire in futuro. In qualche modo l'agente deve essere in grado di comunicare quali siano i parametri che possono essere modificati.

A questo proposito vengono definite le entità:

Object: variabile su cui vengono conservati i valori di stato associati[1].

Management Information Base: struttura dati contenente tutti i possibili SNMP objects di una rete

21.1.4 Management Protocol

Protocollo attraverso il quale dialogano la Management Station e gli SNMP Agent.

query-response: tutto va bene $\longrightarrow$la Management chiede informazioni all'Agent; può modificare parametri a scopi di tuning

SNMP trap: vi sono dei problemi $\longrightarrow$l'agente invia (appena possibile) le informazioni necessarie alla Management. Genralemente le informazioni non sono molto dettagliate. Spetta alla Management indagare più approfonditamente (attraverso query-response)

trap directed polling: interrogazione della Management verso i nodi, uno alla volta, in modo da accertarne il corretto funzionamento (non c'è connessione $\longrightarrow$no acknowledgement sull'avventua comunicazione). In caso di probelmi di comunicazione $\longrightarrow$query-response intensificato.

proxy agent: programma istallato su una macchina "vicina" al dispositivo da monitorare poichè quest'ultimo non può avere SNMP Agent istallato. La comunicazione fra proxy e dispositivo avviene solitamente attraverso un protocollo non standard; il proxy si interfaccia con la Management, in vece del dispositivo, tramite SNMP

sicurezza: dall'SNMPv2c sono state introdotte alcune tecniche di sicurezza, in particolare:

- authentication: attraverso tecniche crittografiche
- privacy: cifratura dei dati (solo se vi è stata autenticazione)

[1] Non è un oggetto nel senso generalmente usato n informatica, in quanto non è dotato di metodi ma solo di campi dati.

21.2 Management Information Structure

21.2.1 Abstract Syntax Notattion 1

L'insieme degli objects definiti costituisce il "cuore" dell'SNMP. E' stato dunque necessario creare uno standard indipendente per avere il corretto funzionamento con dispositivi di tutti i vendor:

- definizione standard (per la quale sarebbe andato bene il C)
- codifica per il trasferimento sulla rete (per la quale il C era troppo oneroso)

21.2.1.1 Standard Object Definition Language

Linguaggio ideato appositamente, è un sottoinsieme dell'ASN, derivata dall'OSI:

- ISO 8824: Data Definition Language
- ISO 8825: Encoding Rules

La codifica è stata ottimizzata per ridurre il numero di bits che viaggiano sulla rete:

- molto esteso
- complesso
- non molto efficiente

molto tempo di CPU viene speso nella codifica e decodifica.

21.2.2 Data Description Language

SI tratta di un linguaggio per la definizione delle variabili, analogamente a quanto è possibile fare in ogni linguaggio di alto livello. Viene utilizzato un sottoinsieme proprio della ASN1.

21.2.2.1 Types

INTEGER: numero con segno

BIT STRING: numero senza segno

OCTET STRING: stringa alfanumerica

NULL: tipo nullo

21.2.2.2 Object Identifier

Si è quindi definito un albero standard, ponendo ogni object standard in un determinato posto. Anche l'SNMP MIB è stato inserito nell'albero, come figlio del "Department of Defense" americano.

Un object viene quindi definito dalle etichette degli archi per cui occorre passare, partendo dalla radice, per arrivarvi, racchiuse fra parentesi graffe (e.g. {1 3 6 1 2 1 ...}).

21.2.3 ASN Transfer Syntax

Descrive le trasformazioni degli objects in seuqnze univoche di bytes per la trasmissione.

21.2.3.1 Basic Encoding Rules

Il metodo di applicazione delle regole è ricorsivo, per facilitare la codifica degli object strutturati. Consiste di quattro campi fondamentali:

1. Identifier (1 byte): 2,1,5
2. Lenght (1 byte)
3. Data Field (n byte)
4. End-Of-Content (se non è presente la lunghezza)

21.3 Protocol

SI costituisce essenzialmente di 6 funzioni per la comunicazione fra Management e Agents:

Get-Request: richiede il valore di una variabile

Get-Next_Request: richiede il valore della prossima variabile (per scorrerle tutte)

Get-Bulk-Request: richiede il valore di una grossa mole di dati, tipicamente una intera tabella

Set-Request: modifica una o più variabili

Inform-Request: messaggio di servizio tra una management ed un'altra, contenente l'informazione di aggiornare una data entry in una local MIB

Snmpv2-Trap: messaggio dall'agente al Management, indicante il verificarsi di un evento

Capitolo 22

VPN-1/FW-1 Useful Line Commands

Capitolo 23

VPN-1/FW-1 Default Communication TCP/IP Ports