

Indice

149
151
154
154
158
158
158
165
172
173
173
177
178
181
197
220
243
243
246
249
249
251
252
252
278
279
280
283
283
288
306
314
314
316
317
317
322

	Introduzione	IX
Capitolo 1	Introduzione alla sicurezza e ai firewall	1
	1.1 L'importanza della sicurezza	2
	1.2 Creazione di una politica di sicurezza	8
	1.3 La ruota della sicurezza di Cisco	11
	1.4 Concetti di base dei firewall	17
	1.5 Reti private virtuali	33
	1.6 Certificazioni di sicurezza Cisco	35
	1.7 Riepilogo	41
	1.8 Guida rapida alle soluzioni	42
	1.9 Domande frequenti	44
Capitolo 2	Introduzione ai firewall Cisco PIX	47
	2.1 Cisco PIX Versione 7.0	48
	2.2 Cosa c'è di nuovo in PIX 7.0?	49
	2.3 Comandi aggiunti in PIX 7.0	50
	2.4 Comandi modificati	50
	2.5 A quali comandi bisogna dire addio?	51
	2.6 Funzionalità del firewall Cisco PIX	51
	2.7 Hardware PIX	68
	2.8 Licenze e aggiornamenti del software	71
	2.9 IP versione 6 (IPv6)	108
	2.10 Riepilogo	116
	2.11 Guida rapida alle soluzioni	119
	2.12 Domande frequenti	120
Capitolo 3	Funzionamento dei firewall Cisco PIX	123
	3.1 I contesti di sicurezza	124
	3.2 Il minimo indispensabile: il traffico in uscita	126
	3.3 Apertura della rete: consentire il traffico in ingresso	141

3.4	ACL in uscita (novità)	149
3.5	ACL a tempo (novità)	151
3.6	NAT Control (novità)	154
3.7	Aggirare la traduzione NAT	154
3.8	Policy NAT	158
3.9	Raggruppamento degli oggetti	158
3.10	Esempio d'uso	165
3.11	Riepilogo	172
3.12	Guida rapida alle soluzioni	173
3.13	Domande frequenti	175
Capitolo 4	Adaptive Security Device Manager	177
4.1	Funzionalità, limiti e requisiti	178
4.2	Installazione, configurazione e avvio di ASDM	181
4.3	Configurazione del firewall Cisco PIX utilizzando ASDM	197
4.4	Configurazione di reti private virtuali utilizzando ASDM	229
4.5	Riepilogo	245
4.6	Guida rapida alle soluzioni	245
4.7	Domande frequenti	246
Capitolo 5	Ispezione delle applicazioni	249
5.1	Nuove funzionalità di Cisco PIX 7.0	249
5.2	Supporto e sicurezza dei protocolli	251
5.3	Ispezione del protocollo per il livello dell'applicazione	255
5.4	Riepilogo	278
5.5	Guida rapida alle soluzioni	279
5.6	Domande frequenti	280
Capitolo 6	Filtraggio, rilevamento delle intrusioni e gestione degli attacchi	283
6.1	Filtraggio del traffico Web e FTP	283
6.2	Rilevamento delle intrusioni nel firewall Cisco PIX	298
6.3	Contenimento e gestione degli attacchi	306
6.4	Riepilogo	314
6.5	Guida rapida alle soluzioni	314
6.6	Domande frequenti	316
Capitolo 7	I servizi	317
7.1	Funzionalità DHCP	317
7.2	Il protocollo PPPoE	322

	7.3	EasyVPN	325
	7.4	Il routing e il firewall Cisco PIX	326
	7.5	Accodamento e politiche	334
	7.6	Riepilogo	335
	7.7	Guida rapida alle soluzioni	335
	7.8	Domande frequenti	337
Capitolo 8		Configurazione dell'autenticazione, dell'autorizzazione e dell'accounting	339
	8.1	Introduzione ai concetti di AAA	341
	8.2	Server AAA	352
	8.3	Configurazione dell'autenticazione a console	352
	8.4	Configurazione dell'autorizzazione all'uso dei comandi	356
	8.5	Configurazione dell'autenticazione a console tramite TACACS+ e RADIUS	361
	8.6	Configurazione dell'autenticazione per il traffico che attraversa il firewall	368
	8.7	Configurazione dell'autorizzazione per il traffico che attraversa il firewall	375
	8.8	Configurazione dell'accounting per il traffico che attraversa il firewall	376
	8.9	Riepilogo	377
	8.10	Guida rapida alle soluzioni	379
	8.11	Domande frequenti	381
Capitolo 9		Gestione di un firewall Cisco PIX	383
	9.1	Configurazione dell'attività di logging	383
	9.2	Configurazione dell'accesso remoto	406
	9.3	Configurazione del protocollo SNMP	417
	9.4	Configurazione della data e dell'ora di sistema	424
	9.5	Riepilogo	432
	9.6	Guida rapida alle soluzioni	436
	9.7	Domande frequenti	437
Capitolo 10		Configurazione di una rete privata virtuale	439
	10.1	Le novità della versione 7.0 del software	440
	10.2	Configurazione di una rete privata virtuale site-to-site	455
	10.3	Accesso remoto: configurazione del supporto per i client VPN Cisco	475
	10.4	Riepilogo	487
	10.5	Guida rapida alle soluzioni	488
	10.6	Domande frequenti	490

