b.SECURITY

FORTINET FIREWALL

› BRENNERCOM AG

brennercom

b.SECURITY

COS'È

È la soluzione di firewalling all-in-one fornita da Fortinet che appartiene alla famiglia di prodotti b.SECURITY di Brennercom; ideale per postazioni remote è facilmente integrabile con altri CPE (customer premise equipment) già installati presso la sede del cliente e offre tutte le performance e le funzionalità desiderate:

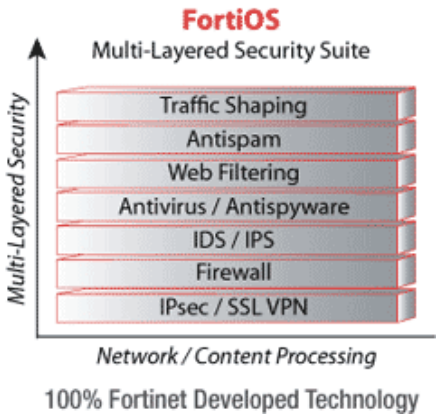
- Servizi attivi IPS-Antivirus;
- Antispam;
- URL filter;
- Application Control.

DESCRIZIONE TECNICA

Le soluzioni di sicurezza FortiGate offrono un'avanzata tecnologia firewall unitamente ad evoluti servizi di sicurezza multi-minaccia, in un'unica piattaforma che consente di contrastare efficacemente eventuali attacchi esterni all'infrastruttura di rete. I dispositivi FortiGate forniscono una protezione completa contro minacce di varia natura, tra cui accessi non autorizzati, tentativi d'intrusione, virus, worm, trojan, spyware, tentativi di phishing, spam e altri tipi di attacchi di tipo content e network based. La soluzione FortiGate risulta essere leader nel settore Unified Threat Management (UTM) grazie anche alla semplicità di gestione e la possibilità di essere inserito in una vasta gamma di scenari di implementazione. Inoltre i servizi di sicurezza FortiGuard ricoprono una vasta gamma di necessità dell'utente finale tra cui supporto tecnico, aggiornamenti Antivirus, Antispam e Web Content Filtering, con l'obiettivo di avere un dispositivo di sicurezza costantemente aggiornato che contrasti con efficacia tutti i tipi di attacchi combinati.

Tutti gli apparati FortiGate sfruttano le potenzialità del sistema operativo proprietario FortiOS. Questo sistema operativo è stato sviluppato ponendo primaria attenzione agli aspetti cruciali della sicurezza e mantenendo, allo stesso tempo, elevate prestazioni ed alta affidabilità. Il FortiOS è un sistema operativo progettato per sfruttare la potenza dei processori di rete e i contenuti dei dispositivi FortiGate.

FortiASIC è infatti la famiglia di processori ad alte prestazioni che offrono una notevole accelerazione dei calcoli intensivi con conseguente aumento delle prestazioni generali degli apparati FortiGate.
Di seguito viene riportata una descrizione più dettagliata di alcuni servizi di sicurezza offerti dal FortiOS.



FIREWALL

La tecnologia di Firewalling Fortinet combina le potenzialità offerte dallo stateful inspection ASIC-accelerated con una serie di motori integrati per la sicurezza applicativa che consentono di identificare e bloccare rapidamente le minacce più complesse. Il Firewall è alla base della soluzione di sicurezza UTM offerta dagli apparati FortiGate, infatti i servizi di protezione e controllo dei flussi sono completamente integrati con le altre funzionalità di sicurezza offerti dalla soluzione FortiGate: VPN, Antivirus, Intrusion Prevention System (IPS) Web Filtering, Antispam e Traffing Shaping.
La tecnologia di firewalling FortiGate introduce quindi una serie di benefici tra cui:

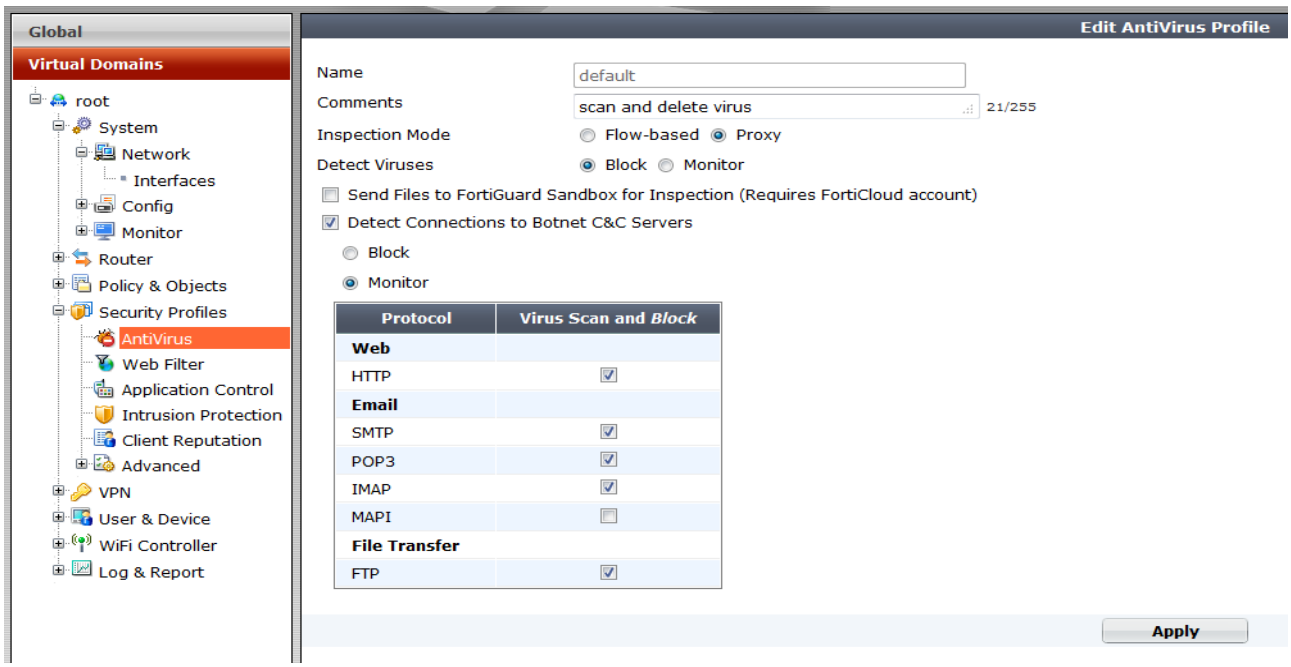
- L'utilizzo dei processori di rete FortiASIC che consentono di ottenere elevatissime prestazioni di firewalling e traffing shaping;
- Un'efficace protezione, attraverso profili di sicurezza e mediante la completa integrazione con le altre tecnologie Fortinet (Antivirus, IPS, ecc.);
- L'applicazione di "full content inspection" per i principali protocolli di rete tra cui HTTP, FTP, SMTP, Post Office Protocol version 3 (POP3), Internet Mail Access Protocol (IMAP), instant messaging (IM), and Network News Transfer Protocol (NNTP);
- La possibilità di definire con semplicità protocolli e applicazioni custom con un elevato grado di granularità nella definizione delle politiche di protezione;
- Le diverse modalità di funzionamento (Transparent, NAT Statico e NAT Dinamico) che consentono un facile adattamento all'infrastruttura di rete e la versatilità nell'implementazione;
- La definizione di domini di sicurezza virtuali e di zone di sicurezza che consentono di suddividere l'apparato in una molteplicità di istanze virtuali dedicate;
- Un semplice inserimento nelle infrastrutture di rete complesse attraverso il supporto dei protocolli di routing dinamico (RIP, OSPF, BGP e PIM);
- La protezione per i servizi VoIP attraverso il supporto dei protocolli H.323, SIP e SCCP;
- L'estensione della protezione firewall anche agli apparati che lavorano fuori dal perimetro di rete grazie all'agent FortiClient di sicurezza per gli end-point;
- Il supporto che consente di abbattere le percentuali dei fuori servizio;
- L'interfacciamento con i sistemi FortiManager e FortiAnalyzer che consentono un controllo centralizzato di tutte le funzionalità firewall e dei dati/eventi di sicurezza rilevati.

UTM BUNDLE

Il bundle UTM (opzionale) introduce le funzionalità di seguito descritte che aumentano il livello di sicurezza dell'intera infrastruttura ICT.

ANTIVIRUS

I sistemi UTM FortiGate consentono l'attivazione (su licenza) di funzionalità Antivirus gateway per il controllo del traffico di rete ed il blocco di virus e malware veicolati dallo stesso. Effettuando un'analisi del traffico di tipo web, mail e file transfer, si offre la possibilità di limitare il range di azione e diffusione del software malevolo al perimetro dell'infrastruttura, andando così a diminuire l'esposizione alle infezioni dell'intero parco macchine. Gli apparati FortiGate utilizzano diversi motori di analisi per poter contrastare al meglio le minacce apportate dai virus. In particolare una prima difesa è rappresentata dall'analisi effettuata attraverso le firme antivirus sviluppate dal centro di ricerca FortiGuard. I tecnici specializzati Fortinet ricercano in maniera continuata nuove minacce virus in diffusione sulle reti del mondo individuando in tempi strettissimi le signature relative ai nuovi virus individuati. Ciò consente di avere un database centralizzato in continuo aggiornamento, che viene distribuito in maniera periodica o su richiesta a tutti gli apparati FortiGate con licenza antivirus. Il motore antivirus quindi consente di individuare, bloccare e mettere in quarantena il traffico contente malware riconosciuto. L'analisi del traffico può essere effettuata in due modalità: Proxy e Flow-based. Nel primo caso viene massimizzata la possibilità di individuazione del malware, attraverso la verifica della presenza di virus polimorfici o artificialmente modificati, nel secondo caso vengono massimizzate le performance, individuando i virus direttamente nel flusso dati passante.



In aggiunta al primo livello di filtraggio, i sistemi FortiGate sono dotati di motori di rilevamento euristico che consentono l'individuazione di traffico sospetto, anche in assenza di una signature relativa. Questo motore consente di intercettare anche malware per cui non è ancora stata individuata la signature. I sistemi FortiGate permettono contestualmente il blocco del traffico diretto alle Botnet ed ai relativi server Command and Control.

In aggiunta a quanto già indicato i sistemi FortiGate implementano i più sofisticati sistemi Sandbox, su macchina locale, macchina dedicata e cloud Fortinet.

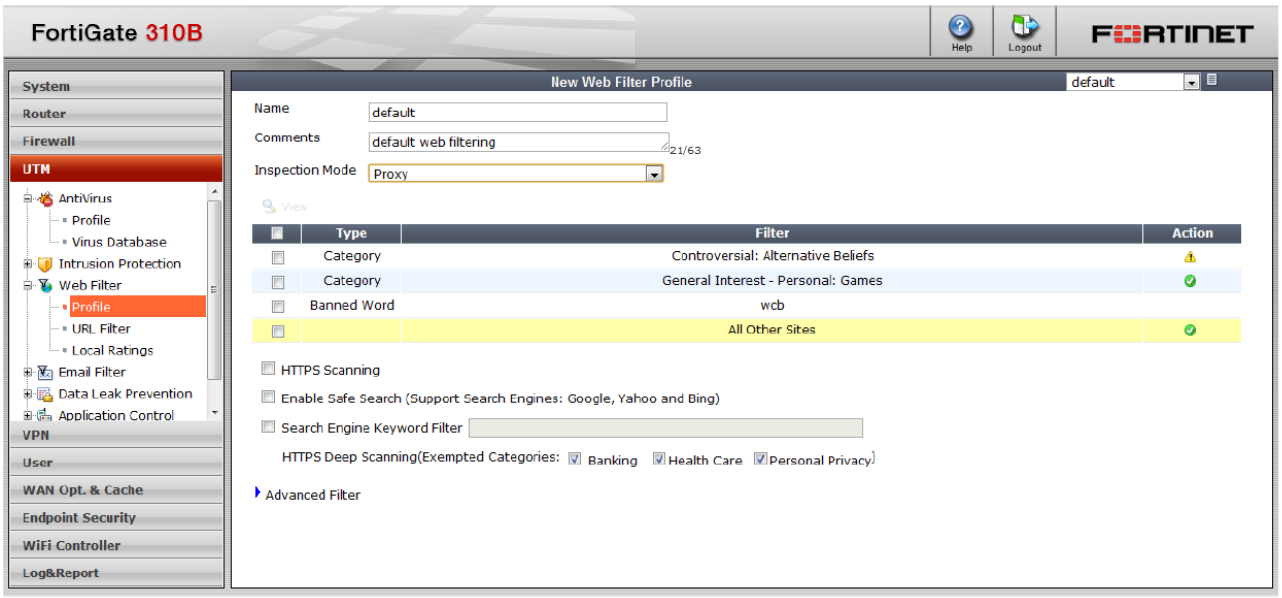
INTRUSION PREVENTION SYSTEM

I sistemi di rilevamento e prevenzione delle intrusioni (IPS, Intrusion Prevention System e Detection) forniti dal servizio FortiGuard di Fortinet mettono a disposizione strumenti di difesa contro attività dannose difficilmente rilevabili in rete. Il servizio FortiGuard Intrusion Prevention fornisce un sistema di rilevamento, allarme e blocco basato su un database personalizzabile contenente un elevato numero di signature conosciute. Questo consente ai sistemi di sicurezza multi-threat FortiGate di bloccare attacchi capaci di eludere i tradizionali sistemi, assicurando una risposta in tempo reale alle minacce e la rapida diffusione delle stesse. Fortinet è in grado di fornire firme di attacco h24 e in tempo reale e grazie alla rete globale FortiGuard, i sistemi FortiGate riescono a bloccare gli attacchi più pericolosi nel perimetro della rete, prima che possano diffondersi all'interno dell'infrastruttura protetta. La tecnologia Fortinet supporta inoltre l'analisi euristica che aggiunge preziose capacità di riconoscimento di comportamenti anomali e che consente di individuare anche attacchi la cui signature non sia ancora stata elaborata e diffusa.

WEB CONTENT FILTERING

Oltre all'utilizzo dalle tradizionali blocking list, la soluzione Web Content Filtering (WCF) integra altre funzioni di sicurezza implementate da FortiGate. Il WCF di Fortinet utilizza un'ampia varietà di azioni per attuare inspection, rate limiting e controllo sul traffico web. Attraverso l'utilizzo della soluzione WCF è possibile filtrare il traffico Web basandosi su:

- Applicazioni utilizzate con blocco completo o parziale e selettivo;
- Contenuti come definiti nelle policy di data loss prevention (DLP);
- Pattern matching su wildcards;
- Multi-language pattern matching;
- Web pattern list.



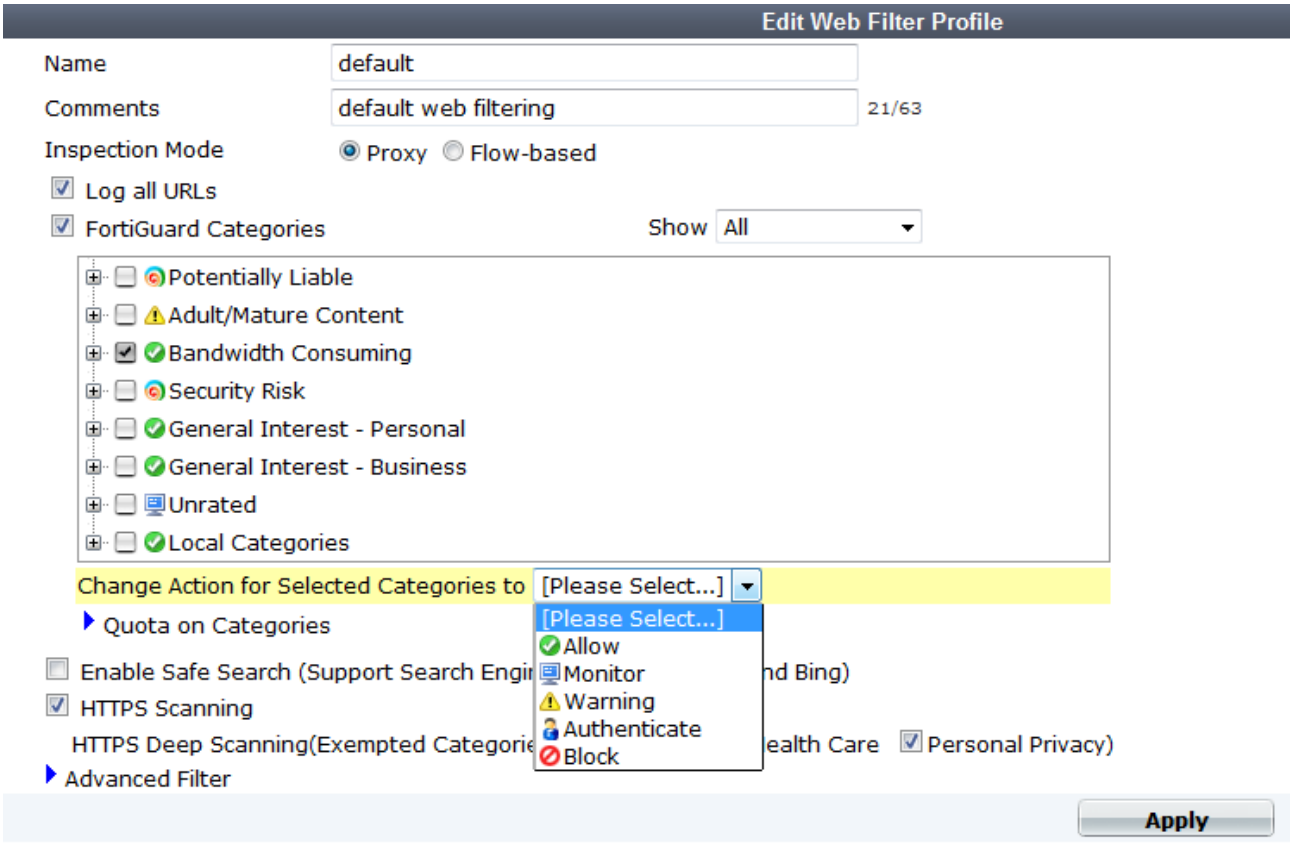
Per incrementare l'efficacia della detection e della prevenzione, i servizi di Web Filtering possono essere combinati con funzioni di Anti Virus, Intrusion Prevention, Anti-Spam, etc…

I firewall FortiGate supportano l'ispezione di HTTPS, evitando quindi il tunneling cifrato utilizzato per mascherare attacchi o utilizzo fraudolento.

Il Web filtering è utilizzato tipicamente per prevenire la navigazione (inappropriata e fuori dalle policy aziendali) su siti pericolosi, da parte degli utenti. Il Web filtering permette agli amministratori di consentire esplicitamente la navigazione o il passaggio di traffico (senza ispezione) verso siti noti e garantiti, in modo da accelerare i flussi di traffico intrinsecamente sicuro.

Il Web filtering permette agli amministratori di customizzare facilmente le liste di URL mediante settaggi locali, attraverso l'utilizzo di stringhe di testo e regular expressions.

Si possono assegnare 6 tipi di azioni sulla base di URL specifica o categorie di URL:



- ALLOW: Consente la navigazione verso il sito richiesto; se richiesto dalla policy di sicurezza, il traffico viene passato ad altre funzioni di sicurezza per una ispezione approfondita dei contenuti;
- BLOCK: Impedisce l'accesso a siti pericolosi o inappropriati riportando un messaggio di warning customizzabile all'utente;
- WARNING: Sottopone un messaggio di warning all'utente per poi consentirne la navigazione consapevole;
- PASS: Consente la navigazione verso il sito richiesto effettuando un bypass delle altre funzioni di sicurezza impostate nella policy. Questa funzione deve essere usata solo per siti completamente affidabili;
- EXEMPT: si comporta come l'azione "Pass" ma l'eccezione alla scansione è rimossa allo scadere della sessione in corso;
- MONITOR: Permette l'accesso e logga l'accesso a siti appartenenti a questa categoria;
- AUTHENTICATE: Richiede una user authentication prima di consentire la navigazione per consentire l'accesso a siti appartenenti a questa categoria o gruppo di categorie.

Il servizio di Web Filtering fornisce informazioni su 77 categorie web, più di 30 milioni di siti e più di 2 miliardi di pagine web, divenendo così leader nell'accuratezza e nel numero di categorie coperte. I firewall FortiGate quindi sono in grado di scansionare, classificare, e filtrare il traffico Web, basandosi su categorie quali:

- POTENZIALMENTE RESPONSABILI: abuso di droga, folklore, hacking, illegalità o non etico, occulto, phishing, plagio, proxy avoidance, razzismo e odio, violenza, traduzioni web;
- CONTROVERSE: aborto, materiale per adulti, gruppi ed organizzazioni, alcohol, gruppi estremisti, gioco d'azzardo, nudità, pornografia, abbigliamento intimo, educazione sessuale, sport di caccia e guerra, cattivo gusto, tabagismo, armi;
- POTENZIALMENTE NON PRODUTTIVE: pubblicità, tradinge brokeraggio, cartoline elettroniche, freeware, downloads, giochi, IM, newsgroup e messaggistica, web chat, email web-based;
- POTENZIALMENTE CONSUMATORI DI BANDA: internet radio e televisione, telefonia internet, download multimediale, file sharing peer-to-peer, personal storage;
- RISCHI DI SICUREZZA POTENZIALI: malware, spyware;
- INTERESSE GENERALE: arte e intrattenimento, educazione infantile, cultura, finanza e banche, organizzazioni generali,

salute e bellezza, ricerca di lavoro, medicina, news e media, relazioni personali, veicoli personali, siti web personali, organizzazioni politiche, immobiliare, referenze, religione, ristoranti, motori di ricerca, shopping e auction, società e stili di vita, sport, viaggi;
- ORIENTATE AL BUSINESS: forze armate, business, organizzazioni legali e governative, information technology, sicurezza informatica e IT;
- ALTRE: server di contenuti, contenuti dinamici, miscellanee, web hosting.

APPLICATION CONTROL

Le funzionalità di Application Control sono un elemento fondamentale per offrire una soluzione completa di sicurezza di tipo content-based. La tecnologia ha introdotto con il Web 2.0, i social media, il cloud computing e la virtualizzazione un aumentato della complessità del traffico di rete, ponendo quindi come requisito la necessità di capire ciò che accade a livello applicativo in una rete. Il FortiOS usa efficienti tecniche di controllo delle applicazioni per fornire un quadro delle applicazioni che generano traffico sulla rete, applicando un controllo che non influisce sulle prestazioni. Una volta resa possibile la caratterizzazione ed il riconoscimento del traffico a livello applicativo, il FortiGate offre la possibilità di bloccare in maniera semplice le applicazioni non consentite ed di controllare tramite le altre funzionalità UTM il traffico applicativo consentito.

Il controllo delle applicazioni effettuato dagli apparati FortiGate non è soltanto limitato al controllo delle porte TCP e UDP utilizzate, ma è portato ad un livello più alto dello stack protocollare. Lavorando a livello applicativo è ad esempio possibile bloccare le applicazioni che funzionano su traffico http senza dover bloccare la porta TCP 80 e di conseguenza l'intera navigazione web. Il controllo delle applicazioni può essere attivato su le varie policy di traffico definite sull'apparato Fortigate ed anche sul traffico cifrato (HTTPS, POP3S, SMTPS, IMAPS) e VPN IPsec e SSL VPN.

È possibile creare più liste di controllo delle applicazioni, ciascuna configurata per consentire, bloccare o monitorare una lista unica di applicazioni. L'elenco delle applicazioni disponibili sono catalogate e controllate dal FortiGuard Application Control Database che è in grado di rilevare più di un migliaio di diverse applicazioni Web, programmi software, servizi di rete e protocolli di traffico. Le categorie di applicazioni definite dal servizio Application Control di Fortinet sono le seguenti: Botnet, Database, Enterprise Applications, File Transfer, Games, Instant Messaging, Internet Protocol, Internet Proxy, Network Backup, Network Services, Peer-to-Peer, Protocol Command, Remote Access, System Update, Video/Audio Streaming, Voice over IP, Web, Web Browser Toolbar e Web-based Email. Il database è costantemente aggiornato tramite il FortiGuard Distribution Network in modo da poter riconoscere le nuove applicazioni e le nuove versioni delle applicazioni esistenti.

ANTISPAM

La tecnologia Antispam di Fortinet offre un'ampia gamma di funzioni per individuare, etichettare, mettere in quarantena e bloccare i messaggi di spam e i loro allegati dannosi. Le piattaforme FortiGate offrono la possibilità di attivare in abbonamento il servizio FortiGuard Antispam integrato come uno degli elementi delle funzionalità di protezione multi-livello.
L'apparato Fortigate utilizza per rilevare e bloccare una vasta gamma di messaggi spam, sia un database di reputazione dell'IP del mittente che un database di firme spam, oltre che sofisticati strumenti di filtraggio, i quali consentono di ridurre drasticamente la quantità di messaggi spam che un server di posta di organizzazione è costretto ad elaborare. La possibilità di configurare politiche personalizzabili consente di applicare il filtraggio antispam su base dominio, gruppo di utenti, e singolo utente ed inoltre la tecnologia di rilevamento dual-pass riduce in modo significativo il volume dello spam a livello perimetrale. Gli aggiornamenti dei database e delle firme vengono continuamente fornite al apparato attraverso la rete di distribuzione globale FortiGuard.

AUTENTICAZIONE

Sui dispositivi FortiGate è possibile utilizzare la funzionalità di Identity Based Policy. Questa funzionalità permette di discriminare il traffico in transito in base a Policy Firewall che tengono conto "dell'identità" della "sorgente"; questo attraverso un meccanismo di autenticazione che può essere scelto tra i seguenti:

- Local database;
- LDAP;
- Radius;
- Tacacs+;

• Active Directory (con Agent o senza);
• eDirectory (con Agent o senza).

La soluzione Fortinet prevede un'integrazione completa con i sistemi aziendali Microsoft Active Directory e Novell eDirectory. Tale integrazione è realizzata grazie al software gratuito Fortinet "FSSO" (Fortinet Single Sign On) che consente e abilita il dialogo e le interrogazioni tra gli apparati FortiGate e la strutture AD e eD. Il sistema permette altresì un'integrazione nativa (senza agent) con MAD (Microsoft Active Directory) per il SSO senza l'utilizzo di NTLN (NT LAN Manager).

NGFW LICENSE

A differenza del bundle UTM, la licenza Next Generation Firewall è espressamente pensata per la protezione dei server e introduce unicamente la funzionalità denominata APPLICATION CONTROL descritta nel precedente paragrafo.

SERVICE LEVEL AGREEMENT

VENDITA

DESCRIZIONE		KASKO [1 Anno]	KASKO [3 Anni]
Orario di risposta (finestra di disponibilità)	lunedì - venerdì	08.00 - 17.00	08.00 - 17.00
	sabato	n.d.	n.d.
	domenica	n.d.	n.d.
	festività naz./reg.	n.d.	n.d.
Presa in carico		immediata	immediata
Tempi di sostituzione hardware		2gg. lavorativi (12 MESI)	2gg. lavorativi (36 MESI)
Finestra di intervento	lunedì - venerdì	08.00 - 17.00	08.00 - 17.00
	sabato	n.d.	n.d.
	domenica	n.d.	n.d.
	festività naz./reg.	n.d.	n.d.
Raggiungibilità Service Desk	Telefono	✓	✓
	e-mail	✓	✓

NOLEGGIO

DESCRIZIONE		KASKO [3 Anni]
Orario di risposta (finestra di disponibilità)	lunedì - venerdì	08.00 - 17.00
	sabato	n.d.
	domenica	n.d.
	festività naz./reg.	n.d.
Presa in carico		immediata
Tempi di sostituzione hardware		2gg. Lavorativi (36 MESI)
Finestra di intervento	lunedì - venerdì	08.00 - 17.00
	sabato	n.d.
	domenica	n.d.
	festività naz./reg.	n.d.
Raggiungibilità Service Desk	Telefono	✓
	e-mail	✓

CONDIZIONI DI FORNITURA

VENDITA

- IVA: 22%;
- Pagamento: 20 gg. data fattura;
- Validità dell'offerta: 60 gg. dalla data della presente;
- La fattura sarà emessa alla conclusione dei lavori e dopo il collaudo dell'apparato.

NOLEGGIO

- Durata minima 36 mesi non modificabile.
- Allo scadere dei 36 mesi di contratto, detto si rinnova tacitamente per ulteriori 12 mesi (e così via di 12 mesi in 12 mesi); la gestione del servizio avverrà come di seguito descritto:
  - HARDWARE&MANUTENZIONE
    - Richiedere la sostituzione dell'HW con un nuovo modello (nuovo contratto);
    - Continuare a utilizzare l'HW presente e godere del servizio di manutenzione per ulteriori 12 mesi (tacito rinnovo) senza variazioni del canone mensile.
  - SOFTWARE (license)
    - Richiedere la dismissione delle licenze;
    - Continuare a utilizzare le licenze (SW) per ulteriori 12 mesi (tacito rinnovo) senza variazioni del canone mensile.

Per ulteriori informazioni consultare le "Condizioni generali di contratto" e le "Commissioni in caso di recesso anticipato", scaricabili alla pagina web: http://www.brennercom.it/it/support/download.

SET-UP BASE FIREWALL

- Spedizione del FW
- Aggiornamento all'ultimo firmware stabile
- Collegamento alla rete di mgmt di Brennercom
- Configurazione accesso Internet (in modalità ANY in uscita)
- Testing del servizio

SET-UP LICENZE (opzionale)

- Registrazione della licenza nel FW
- Configurazione della licenza

La quotazione delle ore necessarie alla configurazione delle licenze dipende dalla quantità di regole configurate nel Firewall (servizio b.PROFESSIONAL - System Integration)

brennercom

BRENNERCOM AG/SPA
Via Pacinotti-Str. 12, I-39100 Bozen/Bolzano
Tel +39 0471 060 111 | fax +39 0471 060 188
www.brennercom.it | info@brennercom.it | free call 800 832 832