

Dokumentnamn		
NSEC FortiGate Whitepaper		
Författare		
NSEC		
Version	Datum	Antal sidor
1.0	2009-06-21	4

FortiGate - Vakten vid ingången till ditt nätverk

FortiGate är en brandvägg som effektivt kontrollerar all trafik till och från ditt nätverk. FortiGate bygger sin lösning på egenutvecklad hårdvara och operativsystem som är mycket effektiv. FortiGate förlitar sig på "ASIC accelererad" hårdvara som ger hög prestanda för virussökning av t ex HTTP-trafik i realtid. Detta gör att lösningen är optimerad för att kontrollera nätverkstrafik och därmed en lösning som påverkar nätverksprestanda minimalt.

En unik funktion med FortiGate är att det är en mycket modulär lösning. Du kan använda den som en brandvägg med de funktioner du behöver, eller så kan du använda den som en transparent skanner för nätverkstrafiken. Många väljer t ex att ansluta FortiGate till befintlig brandvägg och endast utnyttja anti-spam, anti-virus och webfilter funktionerna. Eller så kan du använda den som ett rent intrångsskydd i ditt nät. Valet är ditt! Oavsett vad du väljer så håller lösningen mycket hög nivå och tummar inte på funktioner eller säkerhet.

FortiGate valdes till bästa brandvägg i tidningen Nätverk & Kommunikations stora brandväggstest i nummer 20, 2005.

FortiGate enheten har två alternativ för inkoppling i nätverket; Gateway/router eller transparent brygga. Detta gör det enkelt och smidigt att föra in lösningen. Som transparent brygga behövs ingen förändring i ditt IP-nät överhuvudtaget.

Huvudfunktioner:

Brandvägg & VPN:

- Stateful inspection brandvägg
- VPN (IPSec, PPTP, L2TP)
- SSL VPN
- NAT och Traffic shaping
- Autenticering (LDAP, RADIUS m m)
- Stöder RIP dynamisk routing
- Möjlighet att dela upp enheten i zoner, vilket innebär att enheten kan skydda fler olika nät samtidigt.
- Brandväggen är enkel att stänga av så att lösningen kan användas som ett rent Anti-virus skydd eller intrångsskydd m m. Mycket modulär design.

Dokumentnamn		
NSEC FortiGate Whitepaper		
Författare		
NSEC		
Version	Datum	Antal sidor
1.0	2009-06-21	4

Intrångsskydd och detektion:

- Signaturbaserad intrångsdetektion
- Skydd mot kända intrång, stoppar försök till intrång
- Intrångsdetektion för "misstänkt aktivitet" s k "Anomaly detection"
- Möjlighet att skriva egna regler för intrångsskydd

Virussydd:

- Kontroll av protokollen HTTP, FTP, POP3, SMTP och IMAP
- Blockerar infekterade filer eller sparar dem i karantän
- Möjlighet att blockera farliga filtyper
- Egen snabb sökmotor som utnyttjar plattformen optimalt
- "Push" uppdateringar vid virusutbrott till enheten från FortiNet
- Stoppar även kända Spyware, Adware, Trojaner, Dialers m m.
- Viruskontroll av Instant Messaging (MSN, Yahoo m fl.)
- Karantänfunktion tillsammans med FortiAnalyzer
- Kan dekryptera SSL-sessioner för att även hitta virus i krypterade webbsessioner

Webfiltrering:

- Kategorisering av hemsidor på Internet
- Möjlighet att konfigurera vilka kategorier som ska stoppas eller loggas
- Över 70 kategorier att välja mellan
- Kategorisering sker av FortiNet kontinuerligt
- Möjlighet att själv ange sidor och ord som är bannlysta
- Möjlighet att blockera skript (Active-X och Java)
- Möjlighet till åtkomst av förbjudna kategorier för specifika användare och grupper

Anti-spam:

- Kontroll av innehåll och avsändare som effektivt stoppar skräpposten. Uppdateras i realtid av FortiNet.
- Uppslag mot svartlistade IP-adresser som används för spamutskick (s k RBL & ORDBL)
- "HELO DNS" och "Return e-mail address" kontroll
- Möjlighet att stoppa egna definierade ord med "Regular expressions"
- Möjlighet att stoppa eller tillåta e-post adresser och IP-adresser
- Valbart att stoppa spam, eller flagga med ord i ärenderaden
- Checksummekontroll av mail för effektivare anti-spam funktion

Dokumentnamn		
NSEC FortiGate Whitepaper		
Författare		
NSEC		
Version	Datum	Antal sidor
1.0	2009-06-21	4

Data Leakage Prevention

- DLP funktion som förhindrar känslig intern information att lämna nätverket

WAN acceleration

- WAN acceleration för att öka prestandan på applikationer som skickar trafik över långsmammare WAN-länkar

Proxy cache

- Mellanlagring (cache) av webbsidor som besöks.

Loggning och larm:

- Loggning till syslog
- Loggning till FortiAnalyzer enhet (tillval)
- Larm via e-post
- Stöd för SNMP

Instant Messaging och Peer-to-Peer:

- Innehållskontroll av protokoll för populära Instant Messaging protokoll
- Innehållskontroll av protokoll för populära fildelningsprogram ("P2P", "Peer-to-peer")
- Loggning av Instant Messaging och P2P

Administration:

- Webbläsare och SSH-klient

Redundans/lastbalansering:

- Flera enheter kan klustras för failover och lastbalansering för högre prestanda

Uppdateringar:

- Hämtas automatiskt regelbundet via konfigurerbart schema
- Möjlighet till "push" uppdateringar i realtid vid utbrott

Tillbehör och övriga produkter

- *FortiAnalyzer* tar hand om loggning och rapportgenerering. Dessutom har den funktioner för sårbarhetsanalys av kringliggande nätverk.
- *FortiClient* är en klient (mjukvarua) med VPN, lokal brandvägg, webbfiltrering och anti-virus. Ett perfekt komplement för fjärranvändare som vill ansluta säkert via VPN.
- *FortiManager* administrerar flera brandväggar centralt.

Dokumentnamn		
NSEC FortiGate Whitepaper		
Författare		
NSEC		
Version	Datum	Antal sidor
1.0	2009-06-21	4

- *FortiMail* är en kraftfull anti-spam/anti-virus lösning enbart anpassad för att kontrollera e-post