Rapportage Firewall Quickscan



RAPPORTAGE FIREWALL QUICKSCAN

Snel naar

Klik op een onderdeel om direct naar de juiste plek in de rapportage te gaan. Via “Terug naar overzicht” keer je vanuit ieder hoofdstuk terug naar deze pagina.

Beheerdersaccounts
5 aandachtspunten

Beheer en toegang
5 aandachtspunten

Logging en detectie
6 aandachtspunten

Overige aandachtspunten
3 aandachtspunten

Firewallbeleid
1 aandachtspunt

Vervolg
Van bevindingen naar concrete vervolgstappen

Goed om te weten: dit rapport bevat alle gevonden bevindingen, maar nooit de volledige ruwe firewallconfiguratie. Het geüploade bestand is na verwerking direct verwijderd.

Rapportage Firewall Quickscan

Deze rapportage bevat alle aandachtspunten die tijdens de begeleide controle van de FortiGate-configuratie zijn gevonden. De bevindingen zijn bedoeld om samen met de aanwezige specialist te bespreken en te vertalen naar concrete vervolgstappen.

Privacy en dataminimalisatie: de aangeleverde configuratie is tijdelijk verwerkt voor deze analyse en wordt daarna direct verwijderd. Dit rapport bevat alle gevonden bevindingen, maar nooit de volledige ruwe firewallconfiguratie.

Totaal gevonden	High / Critical	Medium	Low / Info
20	7	7	6

Aanbevelingen

Beheerdersaccounts

Terug naar overzicht

HIGH **Admin-account zonder trusted hosts**

Omgeving/vDOM: Algemeen

Admin-account admin heeft geen trusted hosts ingesteld.

Aanbevolen richting: Beperk admin-toegang met trusted hosts per beheeraccount.

HIGH **Admin-account zonder trusted hosts**

Omgeving/vDOM: Algemeen

Admin-account Fortigate heeft geen trusted hosts ingesteld.

Aanbevolen richting: Beperk admin-toegang met trusted hosts per beheeraccount.

INFORMATIONAL **Pre-login banner is niet ingeschakeld**

Omgeving/vDOM: Algemeen

De pre-login banner is niet ingeschakeld. Dit is vooral een aanbeveling voor duidelijke toegangsvoorwaarden.

Aanbevolen richting: Schakel pre-login-banner in als dit past bij de beheer- en klantafspraken.

INFORMATIONAL **Post-login banner is niet ingeschakeld**

Omgeving/vDOM: Algemeen

De post-login banner is niet ingeschakeld. Dit is vooral een aanbeveling voor duidelijke toegangsvoorwaarden.

Aanbevolen richting: Schakel post-login-banner in als dit past bij de beheer- en klantafspraken.

MEDIUM **Standaard admin-account aanwezig**

Omgeving/vDOM: Algemeen

Het standaard account `admin` is aanwezig.

Aanbevolen richting: Gebruik persoonlijke beheeraccounts en schakel het standaard admin-account uit waar dit operationeel mogelijk is.

Beheer en toegang

Terug naar overzicht

HIGH **Interface staat onveilige beheerprotocollen toe**

Omgeving/vDOM: Algemeen

Interface dmz staat HTTP of Telnet beheer toe.

Aanbevolen richting: Verwijder HTTP en Telnet uit allowaccess en gebruik alleen noodzakelijke beheerprotocollen vanaf beperkte beheerbronnen.

HIGH **Interface staat onveilige beheerprotocollen toe**

Omgeving/vDOM: Algemeen

Interface mgmt staat HTTP of Telnet beheer toe.

Aanbevolen richting: Verwijder HTTP en Telnet uit allowaccess en gebruik alleen noodzakelijke beheerprotocollen vanaf beperkte beheerbronnen.

HIGH **Interface staat onveilige beheerprotocollen toe**

Omgeving/vDOM: Algemeen

Interface lan staat HTTP of Telnet beheer toe.

Aanbevolen richting: Verwijder HTTP en Telnet uit allowaccess en gebruik alleen noodzakelijke beheerprotocollen vanaf beperkte beheerbronnen.

HIGH **WAN-interface staat beheer toe**

Omgeving/vDOM: root

WAN-interface wan1 staat beheerprotocollen toe.

Aanbevolen richting: Verwijder beheerprotocollen van WAN-interfaces, tenzij dit expliciet ontworpen is met trusted hosts, local-in policies en beheerafspraken.

HIGH **WAN-interface staat beheer toe**

Omgeving/vDOM: root

WAN-interface wan2 staat beheerprotocollen toe.

Aanbevolen richting: Verwijder beheerprotocollen van WAN-interfaces, tenzij dit expliciet ontworpen is met trusted hosts, local-in policies en beheerafspraken.

Logging en detectie

Terug naar overzicht

MEDIUM **Security Events zonder aantoonbare profieldekking**

Omgeving/vDOM: root

Policy 2 gebruikt Security Events, maar actieve security-profielen zijn niet aantoonbaar gekoppeld.

Aanbevolen richting: Controleer UTM-status, gekoppelde profielen of profielgroep en hun loginstellingen. Security Events geeft geen volledig sessieoverzicht. Gebruik All Sessions waar verkeersregistratie voor onderzoek of rapportage nodig is.

MEDIUM **Security Events zonder aantoonbare profieldekking**

Omgeving/vDOM: root

Policy 3 gebruikt Security Events, maar actieve security-profielen zijn niet aantoonbaar gekoppeld.

Aanbevolen richting: Controleer UTM-status, gekoppelde profielen of profielgroep en hun loginstellingen. Security Events geeft geen volledig sessieoverzicht. Gebruik All Sessions waar verkeersregistratie voor onderzoek of rapportage nodig is.

LOW **FortiAnalyzer opslag- en retentieadvies**

Omgeving/vDOM: Algemeen

Inventarisatie van actieve policies: All Sessions 0, Security Events 3, uit 0, onbekend 0. Dit zijn aantallen policies, geen gemeten logvolumes.

Aanbevolen richting: Meet GB/dag en de grootste logbronnen per policy en logtype. Stem Analytics- en Archive-retentie en ADOM-opslagverdeling af op rapportages en bewaareisen; Analytics vraagt meer ruimte. Retentieverlaging kan bestaande logs verwijderen en verlaagt de dagelijkse ingest niet. Controleer FortiAnalyzer-forwarding en filters afzonderlijk: policylogging bewijst geen ontvangst. Vermijd max-log-rate als standaardbesparing omdat logs verloren kunnen gaan. De FortiGate-config bevat geen bewijs van FortiAnalyzer-retentie, beschikbare opslag of werkelijke besparing.

LOW **Single CPU core overload logging is niet ingeschakeld**

Omgeving/vDOM: Algemeen

Logging voor overbelasting van een enkele CPU-core is niet ingeschakeld.

Aanbevolen richting: Zet log-single-cpu-high op enable zodat performanceproblemen beter zichtbaar worden.

MEDIUM **Syslog logging ontbreekt of staat uit**

Omgeving/vDOM: Algemeen

Er is geen actieve syslog- of FortiAnalyzer-configuratie gevonden.

Aanbevolen richting: Configureer syslog of FortiAnalyzer logging conform het loggingbeleid.

MEDIUM **FortiAnalyzer logging ontbreekt of staat uit**

Omgeving/vDOM: Algemeen

Er is geen actieve FortiAnalyzer- of syslog-configuratie gevonden.

Aanbevolen richting: Koppel de FortiGate aan FortiAnalyzer of borg centrale logging via syslog.

Overige aandachtspunten

Terug naar overzicht

INFORMATIONAL **Geen DNS-profiel gekoppeld**

Omgeving/vDOM: Algemeen

Er is geen tenant-specifiek of globaal DNS-profiel gevonden. Daardoor kan de analyzer niet bepalen welke DNS-resolvers toegestaan zijn.

Aanbevolen richting: Koppel een DNS-profiel aan de tenant of maak een globaal fallbackprofiel.

MEDIUM **USB auto-install is niet uitgeschakeld**

Omgeving/vDOM: Algemeen

USB auto-install voor configuratie of firmware lijkt niet volledig uitgeschakeld.

Aanbevolen richting: Zet auto-install-config en auto-install-image op disable.

MEDIUM **TLS static key ciphers zijn ingeschakeld**

Omgeving/vDOM: Algemeen

Static key ciphers zijn ingeschakeld of niet aantoonbaar uitgeschakeld.

Aanbevolen richting: Zet ssl-static-key-ciphers op disable.

Firewallbeleid

Terug naar overzicht

LOW **Malicious ISDB deny policies ontbreken**

Omgeving/vDOM: Algemeen

Er zijn niet voor beide richtingen deny policies gevonden voor bekende kwaadaardige Internet Service Database categorieen.

Aanbevolen richting: Overweeg bovenin de policyset expliciete inbound en outbound deny policies voor malicious ISDB-groepen, met logging aan.

Vervolg

Terug naar overzicht

Bespreek de prioriteiten samen met de aanwezige specialist. Daarmee kunnen de bevindingen worden vertaald naar een haalbare volgorde voor verbetering, beheer en eventuele verdieping.