

Firewall quicksan



Firewall quickscan

Deze quickscan geeft een eerste indicatie van aandachtspunten in de aangeleverde FortiGate-configuratie. De scan is bedoeld als startpunt voor gesprek en vervangt geen volledige technische review.

Privacy en dataminimalisatie: de aangeleverde configuratie is tijdelijk verwerkt voor deze analyse en wordt daarna direct verwijderd. Dit rapport bevat bewust alleen een beperkte samenvatting en geen volledige firewallconfiguratie.

Totaal gevonden

101

High / Critical

6

Medium

35

Low / Info

60

Samenvatting

In deze quickscan tonen we alle high/critical aanbevelingen. Van overige aandachtspunten tonen we maximaal twee voorbeelden, zodat je een beeld krijgt van de kwaliteit en beheersbaarheid van de configuratie.

Er zijn nog **93** aanvullende aandachtspunt(en) gevonden die niet volledig in dit quickscanrapport zijn uitgewerkt. Neem contact op met signetbreedband voor een volledige bespreking en een concreet voorstel voor verbetering of beheer.

Aanbevelingen

Firmware en lifecycle

HIGH

Firmware loopt achter op baseline

Omgeving/vDOM: Algemeen

De gedetecteerde firmwareversie ligt onder de firmware intelligence policy.

Aanbevolen richting: Plan een firmware-upgrade naar minimaal 7.2.0. Aanbevolen versie volgens de baseline: 7.4.0.

Beheer en toegang

HIGH

Interface staat onveilige beheerprotocollen toe

Omgeving/vDOM: Algemeen

Interface internal12 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 WAN 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 NMC-MGMT 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 WAN 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 NMC-MGMT 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

LOW

Firewall policy zonder logging

Omgeving/vDOM: root

Policy 17 heeft logging uitgeschakeld.

Aanbevolen richting: Schakel logging in voor toegestane policies, minimaal voor security-relevante en breed toegestane verkeersstromen.

LOW

Firewall policy zonder logging

Omgeving/vDOM: root

Policy 36 heeft logging uitgeschakeld.

Aanbevolen richting: Schakel logging in voor toegestane policies, minimaal voor security-relevante en breed toegestane verkeersstromen.

Vervolg

Wil je de volledige analyse, inclusief technische context en concrete verbetervoorstellen, dan kan signetbreedband de configuratie samen met je doornemen en aangeven welke verbeteringen binnen managed firewallbeheer passen.