Diagnostiker-Familie von boddenberg.de · kostenloses Werkzeug

Windows Firewall Diagnostiker: offene Ports verstehen, Firewall sicher einschalten

Welche Anwendung braucht welchen Port, welche Regel lässt ihn zu, und was passiert, wenn du die Firewall einschaltest? Das Werkzeug beantwortet das, bevor es knallt.

Kostenlos	**Pro**	**Eine EXE**	**Server und Clients**
für die einzelne Maschine	für ganze Flotten, in Vorbereitung	keine Installation, keine Cloud	Windows 10/11, Server 2016+

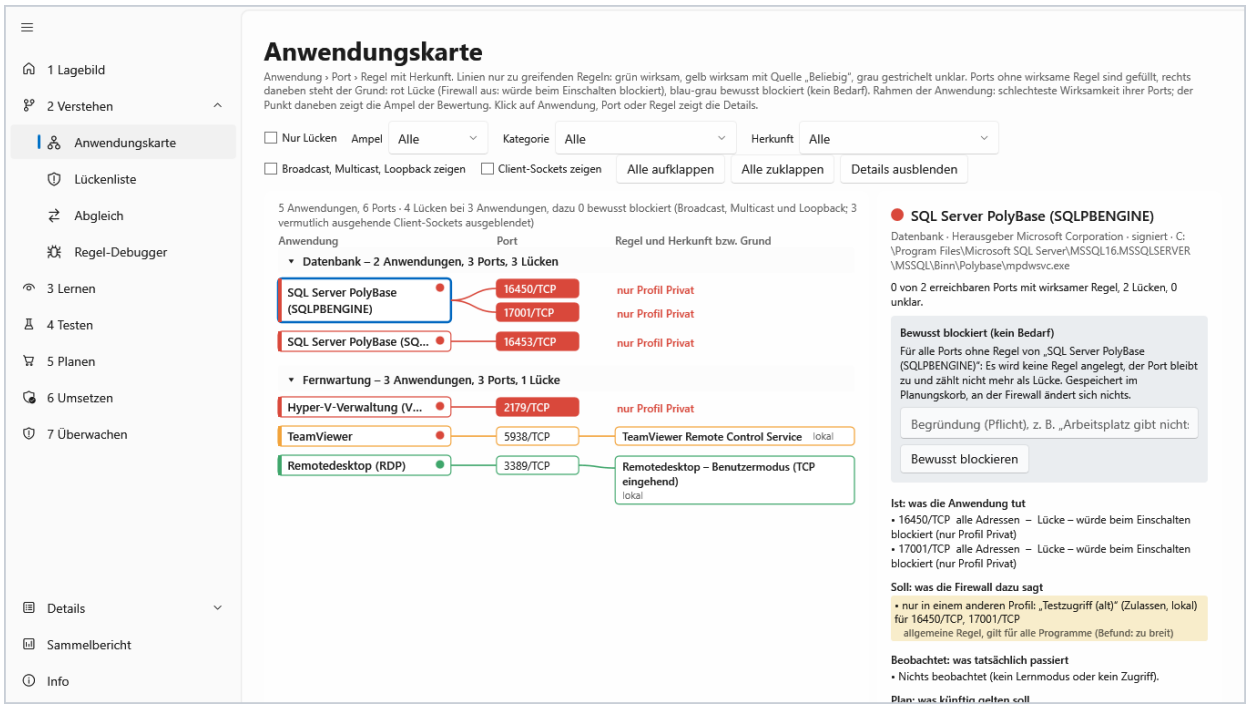
Der Windows Firewall Diagnostiker ist ein kostenloses Diagnosewerkzeug für die Windows-Firewall auf Servern und Clients. Er macht sichtbar, was die Firewall heute tut, und hilft dir, sie ohne Ausfall einzuschalten.

In erstaunlich vielen Organisationen ist die Windows-Firewall abgeschaltet, oft schon seit Jahren und meistens per Gruppenrichtlinie. Das Einschalten scheitert selten an der Technik. Es scheitert an einer einzigen Frage, die niemand sicher beantworten kann: **Was geht kaputt, wenn wir das machen?**

Der Windows Firewall Diagnostiker ist dafür gebaut. Er zeigt je Anwendung, welche Ports offen sind und welche Regel sie freigibt. Er erkennt, ob die Firewall lokal, per GPO oder über Intune gesteuert wird. Und er führt dich in sieben Schritten vom Lagebild bis zur scharfen Firewall: erst beobachten, dann testen, dann umsetzen, jeweils mit Sicherung und Rückweg.

Auf einen Blick

- **Anwendungskarte:** Anwendung › Port › wirksame Regel mit Herkunft (lokal, Name der GPO, Intune).
- **Lückenliste:** alle Ports, die beim Einschalten blockiert würden, mit Grund.
- **Abgleich zentral gegen tatsächlich:** Was kommt aus GPO und Intune, und passt das zu dem, was wirklich lauscht?
- **Lernmodus-Assistent:** Firewall an, eingehend weiter zulassen, protokollieren. Lokal, per GPO oder über Intune.
- **Testregeln mit Ablaufzeit, Planungskorb, Scharfschalten mit Totmannschalter.**
- **Bericht mit Firewall-Ausnahmenregister** als Word, PDF, CSV oder JSON, auch als Sammelbericht über viele Maschinen.
- **Standardmäßig nur lesend.** Alles bleibt auf der Maschine.
- **Zwei Editionen:** kostenlos für die einzelne Maschine, Pro für viele Maschinen, Rollen-GPOs und den Weg nach Intune (in Vorbereitung).



Die Anwendungskarte: Anwendung, Port und die Regel, die tatsächlich greift (konstruierte Beispieldaten)

Warum so viele Windows-Firewalls aus sind

Fragt man nach, hört man fast immer dieselben Geschichten:

- Eine Fachanwendung lief nicht, der Hersteller-Support sagte „Firewall aus", und dabei blieb es.
- Eine alte Gruppenrichtlinie schaltet die Firewall im Domänenprofil ab. Wer sie angelegt hat und warum, weiß niemand mehr.
- Fernwartung, Monitoring, Backup und Softwareverteilung haben ihre Agenten verteilt, und keiner hat dokumentiert, welche davon eingehende Verbindungen brauchen.
- Die Perimeter-Firewall gilt als ausreichend. Intern vertraut man sich.

> **Das eigentliche Risiko**
>
> Ohne Host-Firewall ist jede Maschine von jeder anderen erreichbar, über SMB, RPC, WinRM und RDP. Genau diese Wege nutzen Angreifer und Ransomware nach dem ersten Treffer, um sich seitlich im Netz auszubreiten. Die Perimeter-Firewall sieht diesen Verkehr nicht einmal.
>
> Eine eingeschaltete Windows-Firewall, die eingehende Verbindungen auf das Nötige beschränkt, ist eine der wirksamsten Härtungsmaßnahmen überhaupt. Und sie kostet nichts: Sie ist auf jeder Windows-Maschine schon da.

Dass trotzdem niemand rangeht, ist verständlich. Ein Krankenhaus, ein Produktionsbetrieb oder eine Verwaltung kann sich keinen Montagmorgen leisten, an dem die Fachanwendung steht, weil ein Port fehlt, den nie jemand dokumentiert hat. Was fehlt, ist kein Mut, sondern ein Lagebild und ein Rückweg.

Was der Windows Firewall Diagnostiker ist, und was nicht

Der Windows Firewall Diagnostiker ist ein Analyse- und Einführungswerkzeug für die eingebaute Windows-Firewall. Er läuft als einzelne EXE direkt auf der Maschine, die du untersuchst, mit Oberfläche oder per Kommandozeile. Er verbindet drei Sichten, die sonst niemand zusammenbringt:

Sicht	Frage	Woher die Daten kommen
Ist	Was lauscht auf welchem Port, und welcher Prozess, Dienst oder welches Programm steckt dahinter?	Erfassung auf der Maschine
Soll	Welche Regel lässt den Port zu, in welchem Profil, für welche Quelle, und woher kommt sie?	Windows-Firewall, GPO, Intune
Beobachtet	Wer greift tatsächlich zu, und was wird geblockt?	Firewall-Protokoll im Lernmodus bzw. nach dem Scharfschalten
Plan	Was soll künftig dauerhaft gelten, mit Begründung?	deine Entscheidungen im Planungskorb

Was das Werkzeug bewusst nicht ist

- **Keine zentrale Firewall-Konsole und kein Agent.** Es läuft dort, wo du es startest, und hinterlässt keinen Dienst.
- **Kein Ersatz für dein EDR oder die Perimeter-Firewall.** Es macht die Host-Firewall beherrschbar, die du ohnehin hast.
- **Kein Automat, der Regeln für dich erfindet.** Beobachtet ist nicht freigegeben. Das Werkzeug schlägt vor, du entscheidest.

Der Ablauf: sieben Schritte bis zur scharfen Firewall

Die Navigation des Werkzeugs ist der Ablauf selbst. Jeder Schritt beantwortet eine Frage. Ändernde Schritte zeigen vorher alle Aktionen, verlangen eine ausdrückliche Bestätigung und sichern vorher die komplette Firewall-Konfiguration.



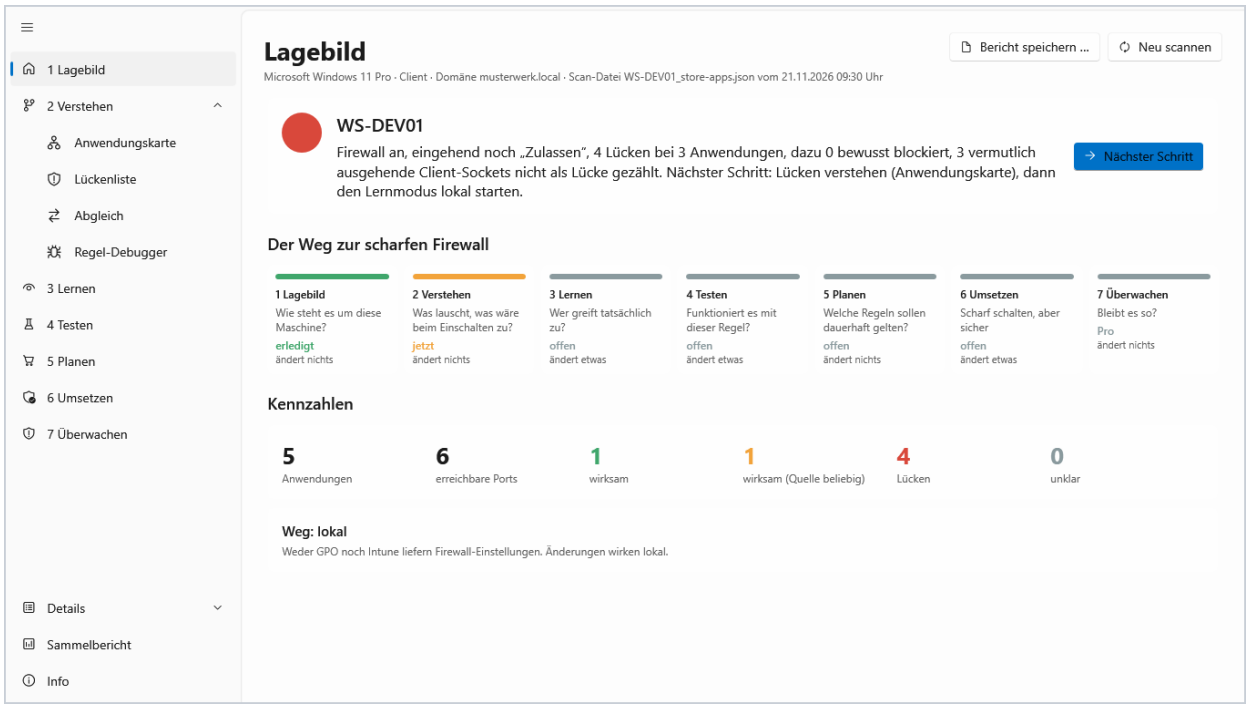
Vom Lagebild bis zur Überwachung nach dem Scharfschalten

Schritt	Frage	Ändert etwas?
1 Lagebild	Wie steht es um diese Maschine, und was ist der nächste Schritt?	nein
2 Verstehen	Was lauscht, welche Regel greift, und was wäre beim Einschalten zu?	nein
3 Lernen	Wer greift tatsächlich zu?	ja: Firewall an, eingehend zulassen, protokollieren
4 Testen	Funktioniert es mit dieser Regel?	ja: Testregeln, die sich selbst wieder entfernen
5 Planen	Welche Freigaben sollen dauerhaft gelten?	nein
6 Umsetzen	Scharf schalten, aber sicher	ja, mit Sicherung, Totmannschalter und Rückweg
7 Überwachen	Was wird jetzt geblockt?	nein

Alle Bildschirmfotos auf dieser Seite zeigen konstruierte Beispieldaten einer fiktiven Maschine.

1 Lagebild: Wo stehen wir?

Die Startseite fasst die Lage in einem Satz zusammen: Ist die Firewall an oder aus, wer steuert sie, wie viele Anwendungen hätten beim Einschalten ein Problem, und was ist der nächste sinnvolle Schritt? Darunter stehen die Kennzahlen und der Fortschritt über die sieben Schritte. Wenn du nur wissen willst, ob du handeln musst, bist du hier fertig.



Lagebild mit Kennzahlen und nächstem Schritt

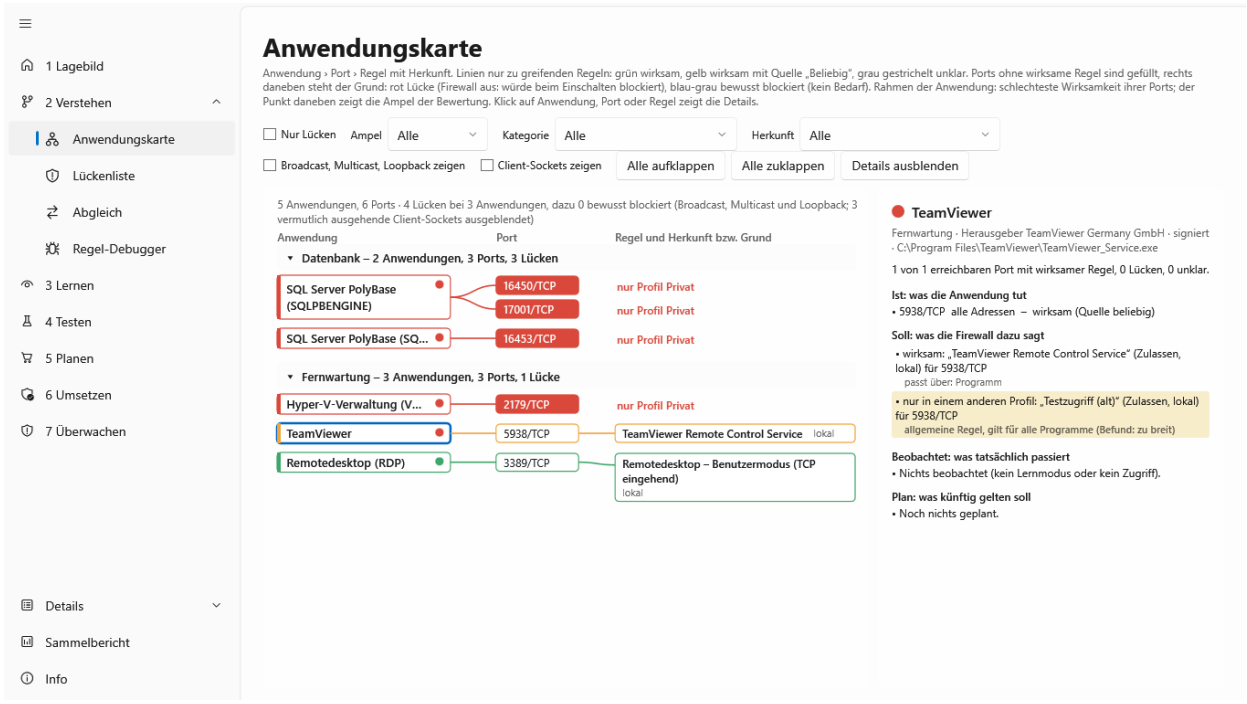
2 Verstehen: die Anwendungskarte

Das Herzstück. Links steht die Anwendung, in der Mitte ihre Ports, rechts die Regel, die tatsächlich greift, samt Herkunft: lokal, Name der GPO oder Intune. Die Herkunft liest das Werkzeug aus der GPO-Liste der Maschine und der zwischengespeicherten Registry.pol, ohne Netzwerkzugriff. Anwendungen sind nach Kategorien gruppiert (Datenbank, Fernwartung, Monitoring, Backup …), Windows-Bestandteile sind zugeklappt, damit die Fremdanwendungen mit Lücken oben stehen.

So liest du die Karte

- **Grün:** Eine Regel lässt zu, die Quelle ist eingeschränkt.
- **Gelb:** Eine Regel lässt zu, aber aus „Beliebig" oder als allgemeine Regel, die für alle Programme gilt.
- **Rot:** keine wirksame Regel. Bei abgeschalteter Firewall heißt das „Lücke – würde beim Einschalten blockiert", bei eingeschalteter „wird blockiert (keine Freigabe)". Daneben steht der Grund: keine Regel, nur Profil Privat, Regel deaktiviert, Block-Regel.
- **Blau-grau:** bewusst blockiert, weil kein Bedarf besteht, mit Begründung.
- **Grau gestrichelt:** nicht sicher bestimmbar. Das Werkzeug schönt nichts. Was unklar ist, bleibt unklar.

Ein Klick auf eine Anwendung öffnet rechts die Details in vier Schichten: Was tut die Anwendung (Ist), was sagt die Firewall dazu (Soll), was wurde beobachtet, und was ist geplant. Im Beispiel unten fällt sofort auf, dass die Freigabe für die Fernwartung zwar wirkt, aber aus „Beliebig", und dass eine alte Testregel nur im falschen Profil existiert und für alle Programme gilt.



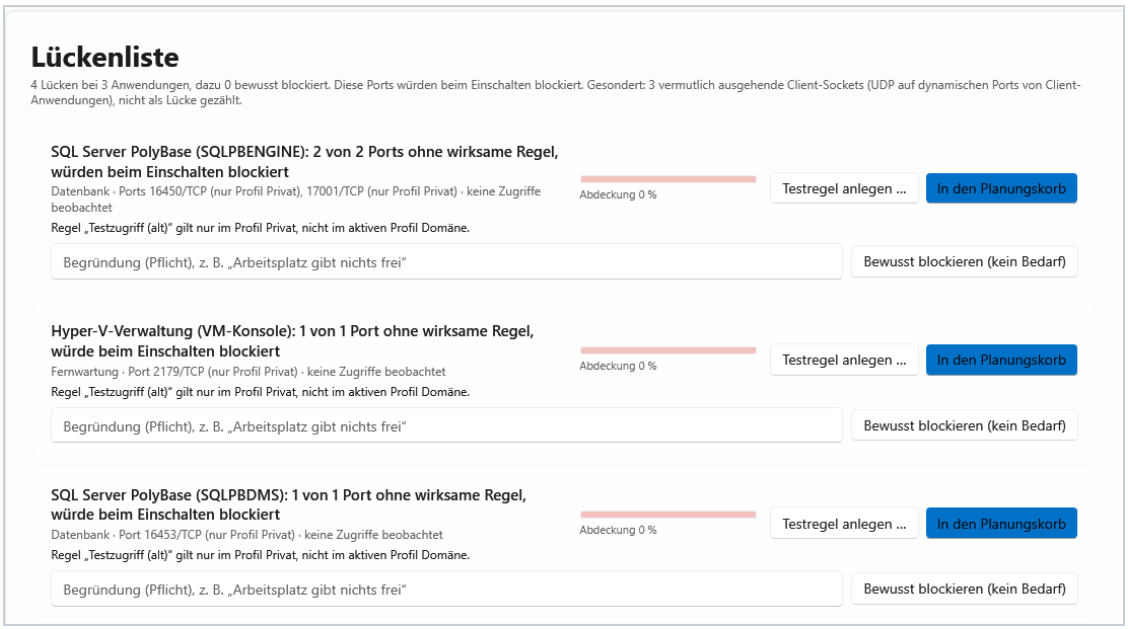
Anwendungskarte mit Detailansicht: Ist, Soll, Beobachtet und Plan einer Anwendung

Typischer Fund: die Regel im falschen Profil

Viele Installer legen ihre Freigabe nur für „Privat“ oder „Öffentlich“ an. Solange die Firewall im Domänenprofil aus ist, merkt das niemand. Nach dem Einschalten ist der Port zu, obwohl „doch eine Regel da ist“. Die Anwendungskarte zeigt solche Fälle rot mit dem Grund „nur Profil Privat“.

2 Verstehen: Lückenliste

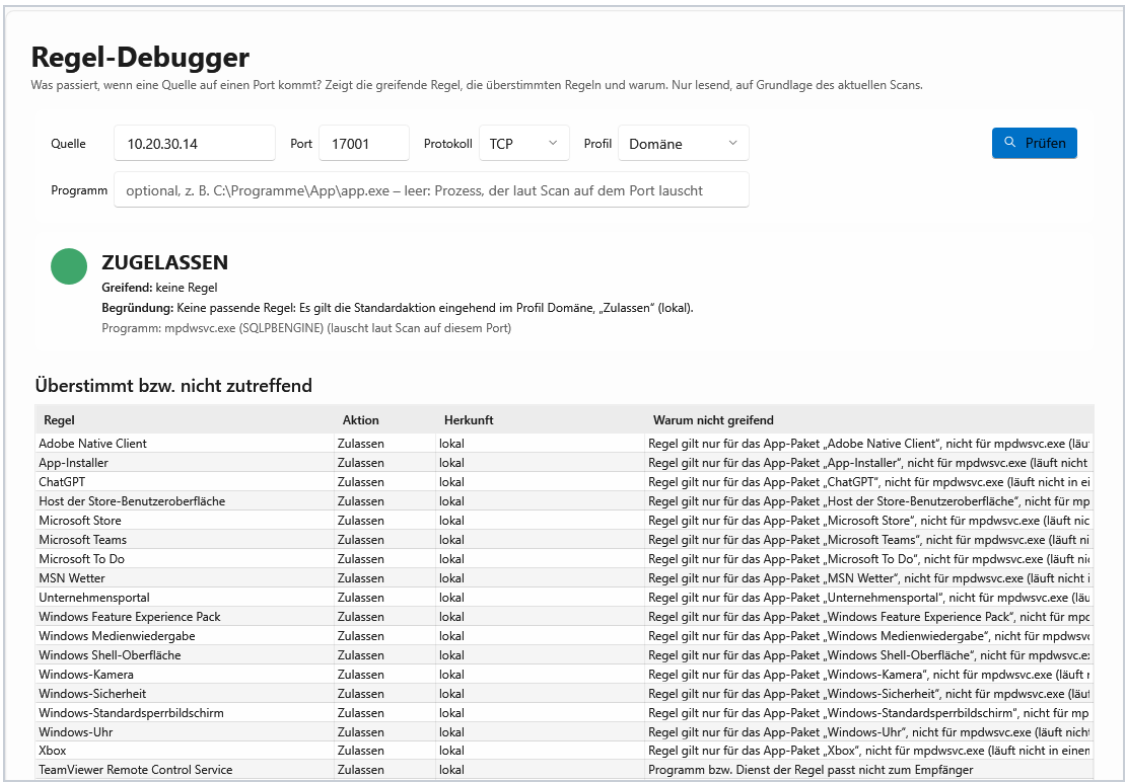
Alle Ports ohne wirksame Regel, sortiert nach Anwendung und mit Grund. Je Eintrag geht es mit einem Klick weiter zur Testregel oder in den Planungskorb. Was niemand braucht, etwa SMB oder die Druckwarteschlange auf einem Arbeitsplatz, markierst du als „bewusst blockiert (kein Bedarf)“, mit Pflicht-Begründung. Auf Clients schlägt das Werkzeug solche Kandidaten vor, auf Servern bewusst nie.



Lückenliste mit Grund je Port

2 Verstehen: Regel-Debugger

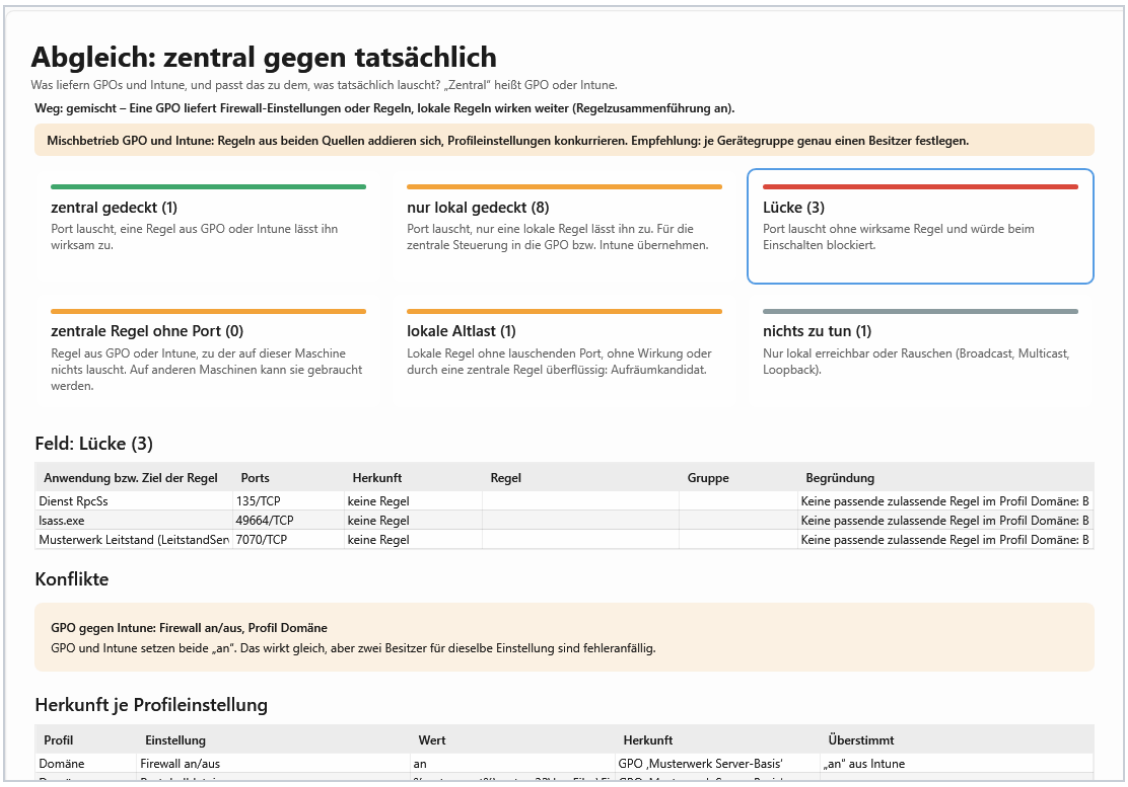
Warum ist dieser Port offen oder zu? Du gibst Quelle, Port, Protokoll und Profil ein und bekommst die greifende Regel, die überstimmten Regeln und eine Begründung in Klartext: „Block gewinnt", „Regel nur im Profil Privat" oder „gilt nur für das App-Paket von Teams, nicht für diesen Dienst". Das ist die Grundlage für jedes Gespräch mit Fachabteilung und Hersteller. Den Debugger gibt es auch auf der Kommandozeile, live oder gegen eine gespeicherte Scan-Datei.



Regel-Debugger mit Begründung je Regel

2 Verstehen: Abgleich zentral gegen tatsächlich

Welche Einstellungen und Regeln kommen aus welcher Gruppenrichtlinie oder aus Intune, und passt das zu dem, was auf der Maschine tatsächlich lauscht? Der Abgleich ordnet jeden Port einem von sechs Feldern zu, von „zentral freigegeben und gebraucht“ bis „lauscht, aber nirgends freigegeben“. Dazu kommt eine Konfliktliste: zwei GPOs mit widersprüchlichen Einstellungen, GPO und Intune gleichzeitig, lokale Regeln, die wegen der Gruppenrichtlinie gar nicht wirken.



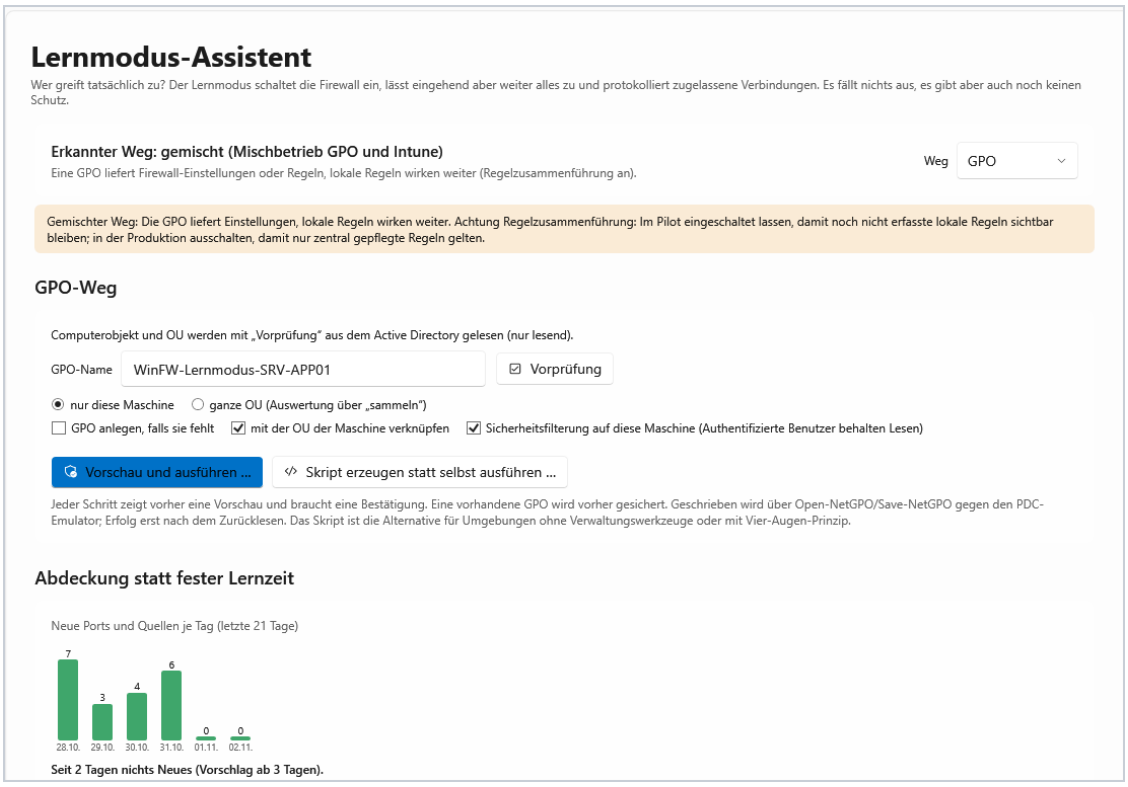
Abgleich zentral gegen tatsächlich, mit Konfliktliste

3 Lernen: erst beobachten, dann entscheiden

Im Lernmodus ist die Firewall an, lässt eingehend aber weiter alles zu und protokolliert jede Verbindung. Es wird also nichts blockiert, aber alles sichtbar. Der Assistent erkennt selbst, welcher Weg passt, und führt dich durch genau die nötigen Schritte:

- **Lokal:** Das Werkzeug setzt die Einstellungen selbst und prüft mit einem Selbsttest, ob das Protokoll wirklich geschrieben wird („Protokoll läuft, letzter Eintrag vor 4 Minuten“). Ein häufiger Stolperstein ist ein eigener Protokollpfad, auf den der Firewall-Dienst nicht schreiben darf.
- **Per GPO:** Auf ausdrücklichen Wunsch legt der Assistent eine Lern-GPO an, verknüpft sie mit der OU der Maschine, beschränkt sie per Sicherheitsfilterung auf diese eine Maschine, schreibt die Einstellungen gegen den PDC-Emulator und liest sie zurück. Alternativ erzeugt er ein Skript für die GPO-Verwaltung.
- **Über Intune:** Der Assistent nennt die nötigen Einstellungen der Richtlinie, die du in Intune setzt.

Wie lange gelernt wird, gibt keine feste Frist vor, sondern die **Abdeckungskurve**: Sie zeigt, wann keine neuen Zugriffe mehr dazukommen. Willst du Monatsabschlüsse, Backup-Läufe und den Patchday dabeihaben, plan rund vier Wochen ein.



Lernmodus-Assistent mit Weg-Erkennung und Abdeckungskurve

4 Testen: Regeln, die sich selbst wieder abräumen

Aus der Karte oder der Lückenliste legst du mit einem Klick eine Testregel an. Testregeln stehen in einer eigenen Gruppe, haben eine Ablaufzeit und werden von einer Aufräumaufgabe wieder entfernt. So kannst du mit der Fachabteilung prüfen, ob eine Anwendung mit genau dieser Freigabe läuft, ohne dass Testreste für immer im Regelwerk kleben. Das geht dort, wo lokale Regeln wirken, also auch bei zentral gesteuerten Firewalls, solange die Regelzusammenführung erlaubt ist.

5 Planen: der Planungskorb

Im Planungskorb sammelst du, was dauerhaft gelten soll: Anwendung, Ports, Quelle, Begründung, verantwortliche Person, Ablaufdatum. Vorschläge aus dem Lernprotokoll landen hier nicht automatisch, denn **beobachtet ist nicht freigegeben**. Aus dem Korb wird entweder lokal angewendet oder ein PowerShell-Skript für die GPO erzeugt, das vorher erhöhte Sitzung, Bearbeitungsrecht und Wirkungsbereich prüft und Erfolg erst nach dem Zurücklesen meldet.

6 Umsetzen: scharf schalten mit Totmannschalter

Beim lokalen Weg schaltet das Werkzeug die Standardaktion eingehend auf „Blockieren", aber nie ohne Netz und doppelten Boden:

- Vorher wird die komplette Firewall-Konfiguration gesichert.
- Pflichtregeln für RDP und WinRM aus dem Admin-Netz und für ICMP-Echo werden gesetzt. Kommt deine eigene RDP-Sitzung nicht aus dem Admin-Netz, bricht das Werkzeug ab, bevor du dich aussperrst.
- Ein **Totmannschalter** als geplante Aufgabe stellt die Sicherung automatisch wieder her, wenn du nicht innerhalb der gewählten Zeit bestätigst, auch wenn die RDP-Sitzung abreißt.
- Schlägt ein Schritt fehl, wird die Sicherung sofort wiederhergestellt.

Steuern GPO oder Intune die Profileinstellungen, ist lokales Scharfschalten gesperrt. Dann gehört die Umsetzung in die zentrale Richtlinie, und das Werkzeug liefert dafür das Skript.

7 Überwachen: Was wurde geblockt?

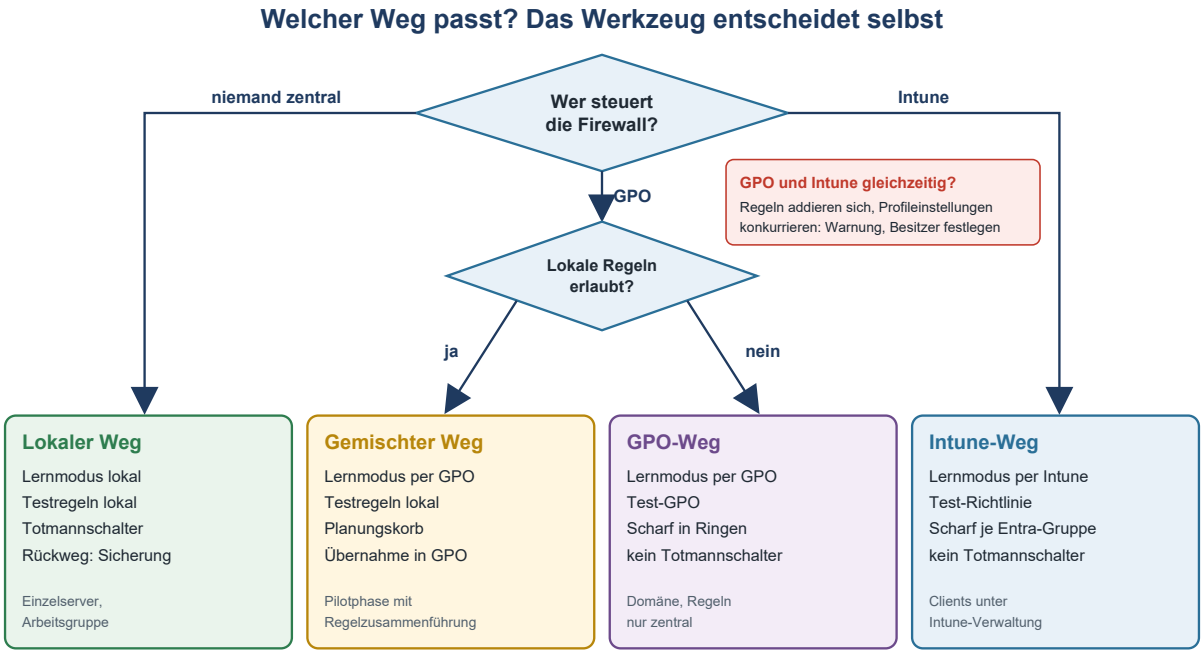
Nach dem Scharfschalten zählt die Gegenrichtung. Das Werkzeug wertet die verworfenen Verbindungen aus dem Firewall-Protokoll aus, je Port, Protokoll und Quellnetz, mit „zuerst gesehen“, „zuletzt gesehen“ und der wahrscheinlichen Anwendung. Vergessene Anwendungen fallen so in Stunden auf statt über Störungsmeldungen. Rauschen wie Broadcast, Multicast und Erkennungsdienste zählt nicht mit.



Auswertung geblockter Verbindungen

Wer steuert die Firewall? Lokal, GPO oder Intune

Ob eine Änderung überhaupt wirkt, hängt davon ab, wer die Firewall steuert. Das ist der Punkt, an dem die meisten Einschaltversuche verwirrend werden: Man setzt lokal etwas, und nichts passiert. Der Windows Firewall Diagnostiker prüft das vor jedem ändernden Schritt und wählt den passenden Weg.



Lokaler Weg, gemischter Weg, GPO-Weg und Intune-Weg

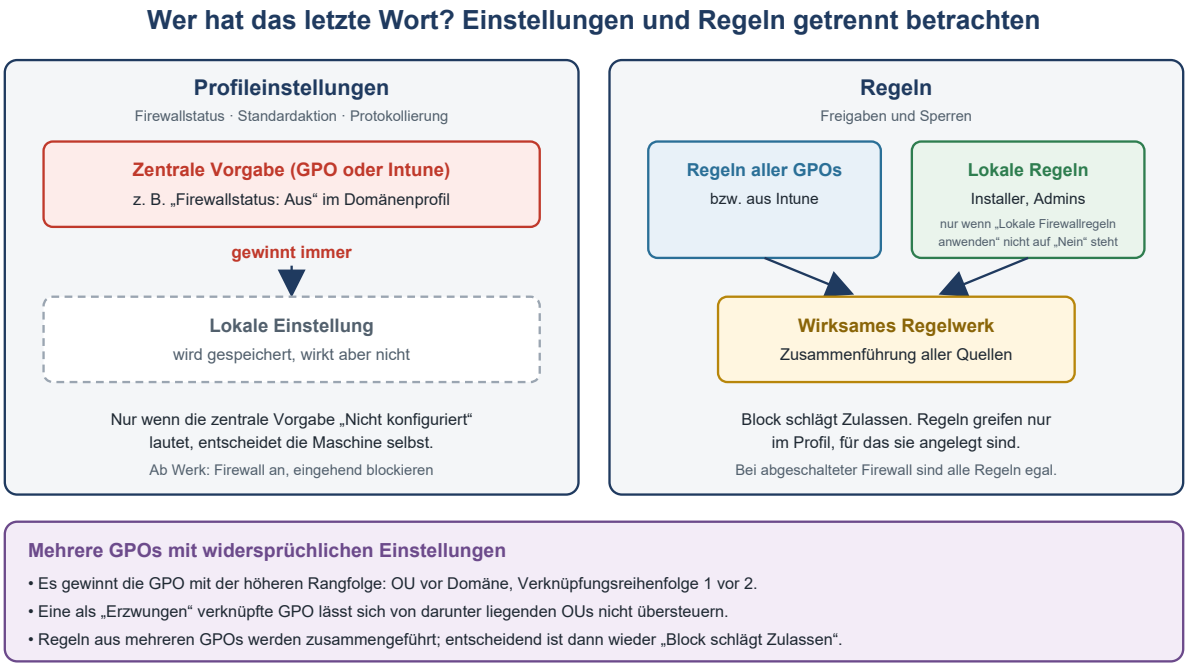
Einstellungen und Regeln folgen unterschiedlichen Spielregeln

Für das Verständnis hilft eine Trennung, die in kaum einer Dokumentation sauber steht:

- **Profileinstellungen** (Firewallstatus, Standardaktion eingehend und ausgehend, Protokollierung): Hier gewinnt die zentrale Vorgabe. Setzt eine GPO „Firewallstatus: Aus“, ist die

Firewall in diesem Profil aus, egal was lokal eingestellt ist. Ein lokales Einschalten wird gespeichert, wirkt aber nicht.

- **Regeln** werden zusammengeführt: die Regeln aller GPOs (bzw. aus Intune) plus die lokalen Regeln, sofern „Lokale Firewallregeln anwenden“ nicht auf „Nein“ steht. Im Regelwerk gilt: Block schlägt Zulassen, und eine Regel greift nur in dem Profil, für das sie angelegt ist.



Wer hat das letzte Wort? Profileinstellungen und Regeln

Vorsicht: „GPO raus“ ist kein Plan

Hängt die Firewall nur an einer „Aus“-GPO, ist die Versuchung groß, die Verknüpfung einfach zu entfernen. Dann gilt beim nächsten Richtlinienabgleich, spätestens nach rund 90 Minuten, wieder die lokale Einstellung, und die steht ab Werk auf **Ein** mit „eingehend blockieren“. Alle Maschinen unter dieser OU schalten gleichzeitig scharf. Was keine Freigabe im richtigen Profil hat, ist weg.

Besser: eine zweite GPO mit höherer Rangfolge für eine Pilotgruppe, zuerst im Lernmodus. Die alte „Aus“-GPO bleibt bis zum Schluss stehen und wird erst entfernt, wenn alle Maschinen über die neue GPO laufen.

Die Fallstricke bei mehreren GPOs

- **Rangfolge:** Bei widersprüchlichen Einstellungen gewinnt die GPO, die zuletzt angewendet wird: OU vor Domäne, und an derselben OU die kleinere Verknüpfungsreihenfolge.
- **Erzwungen:** Ist die „Aus“-GPO als „Erzwungen“ verknüpft, kann eine GPO an einer darunter liegenden OU sie nicht übersteuern. Dann hilft nur, Pilotmaschinen per Sicherheitsfilterung aus der alten GPO herauszunehmen.
- **Zwei Stellen für „aus“:** Die Firewall lässt sich im Knoten „Windows-Firewall mit erweiterter Sicherheit“ und in den älteren administrativen Vorlagen abschalten. Die neue GPO sollte dieselbe Stelle verwenden, sonst wird es undurchsichtig.
- **Nur ein Profil aus:** Häufig ist nur das Domänenprofil abgeschaltet, Privat und Öffentlich sind an. Startet ein Server, bevor er einen Domänencontroller erreicht, landet er kurz im Profil „Öffentlich“,

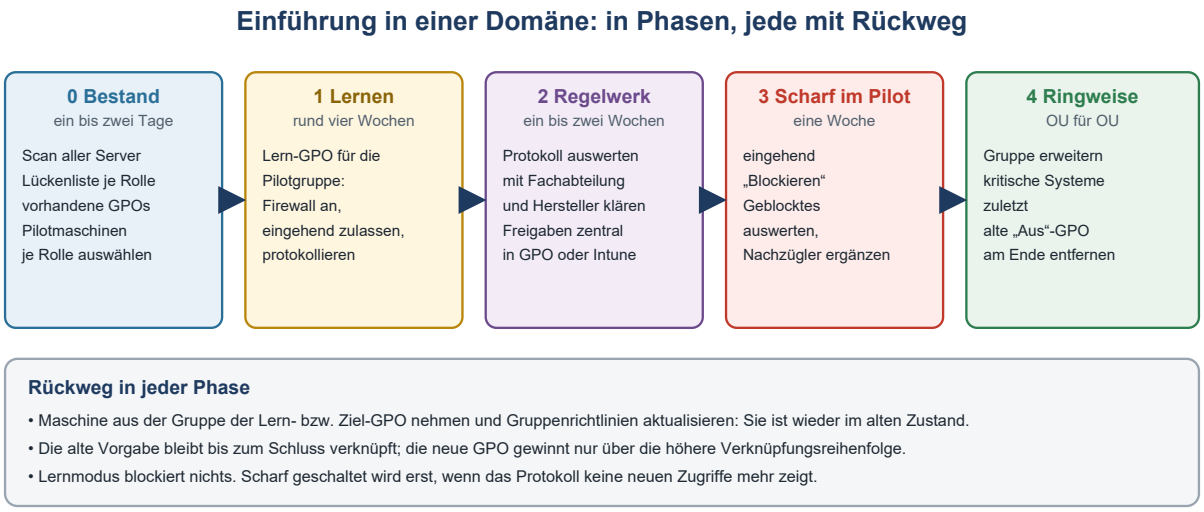
und dort greift die Firewall schon heute. Das erklärt manches „nach dem Neustart geht Dienst X erst nach ein paar Minuten“.

- **GPO und Intune gleichzeitig:** Mischbetrieb ist eine Quelle schwer erklärbarer Effekte. Das Werkzeug warnt davor.

Welche GPO bei einer Maschine tatsächlich gewinnt, zeigen der Abgleich im Werkzeug und ergänzend „gpresult /h“.

Praxis: die Firewall in einer Domäne einschalten

So sieht ein bewährtes Vorgehen aus, wenn die Firewall per Gruppenrichtlinie abgeschaltet ist. Die Phasen sind bewusst klein geschnitten: Jede lässt sich für eine einzelne Maschine zurückdrehen, und es gibt keinen Tag X für alle.



Einführung in Phasen: Bestand, Lernen, Regelwerk, Pilot, Ringe

Phase 0: Bestand

Scan auf allen Servern per Kommandozeile, Ergebnisse auf eine Freigabe, daraus ein Sammelbericht. Danach weißt du, welche Rollen es gibt, wo die meisten Lücken liegen und welche GPOs die Firewall heute beeinflussen. Je Rolle wählst du eine Pilotmaschine aus. Kritische Systeme wie Domänencontroller, PKI oder Klinik- und Produktionssysteme kommen zuletzt.

Phase 1: Lern-GPO für die Pilotgruppe

Eine neue GPO, verknüpft an derselben OU wie die alte „Aus“-GPO, aber mit höherer Rangfolge (Verknüpfungsreihenfolge 1). Sicherheitsfilterung auf eine Gruppe, in der nur die Pilotmaschinen stehen. „Authentifizierte Benutzer“ verlieren dabei nur das Recht „Übernehmen“, das Leserecht bleibt. Eingestellt wird nur das Profil, das heute aus ist:

Einstellung (Domänenprofil)	Wert
Firewallstatus	Ein
Eingehende Verbindungen	Zulassen (Lernmodus, blockiert nichts)
Ausgehende Verbindungen	Zulassen
Protokollierung	verworfene und erfolgreiche Verbindungen, 32.767 KB, Standardpfad

Einstellung (Domänenprofil)	Wert
Lokale Firewallregeln anwenden	Ja (damit Testregeln wirken)

Neue Gruppenmitgliedschaften von Computern greifen erst mit einem neuen Kerberos-Ticket. Ohne Neustart geht das so:

```
klist -li 0x3e7 purge
gpupdate /force
```

Ab Version 2.1 erkennt das Werkzeug einen per GPO gesetzten Lernmodus selbstständig und liefert zwei geplante Aufgaben als Gruppenrichtlinien-Einstellungen mit: eine, die das Protokoll alle 15 Minuten verdichtet, bevor es überläuft, und einen täglichen Scan auf die Freigabe. Der Sammelbericht zeigt dann je Maschine Lernzeitraum und Abdeckungskurve.

Phase 2: Regelwerk

Lückenliste, Lernprotokoll und Regel-Debugger zeigen, was tatsächlich gebraucht wird. Unklare Fälle klärst du mit Fachabteilung und Hersteller, getestet wird mit Testregeln. Was dauerhaft gelten soll, kommt in den Planungskorb und von dort in die zentrale Richtlinie: eine Basis-GPO für alle Server und Rollen-GPOs an den Unter-OUs, etwa für Datenbank- oder Dateiserver.

Phase 3: Scharf im Pilot

In der Lern-GPO wird „Eingehende Verbindungen“ auf „Blockieren“ gestellt. Eine Woche lang zeigt „Was wurde geblockt?“, ob etwas vergessen wurde. Nachzügler-Regeln landen in der zentralen Richtlinie.

Phase 4: ringweise ausrollen

Die Gruppe wächst OU für OU. Sind alle Maschinen drin, wird die alte „Aus“-GPO entfernt und die neue zur regulären Vorgabe, dann ohne Gruppenfilterung. Der Rückweg ist in jeder Phase derselbe: Maschine aus der Gruppe nehmen, Gruppenrichtlinien aktualisieren, fertig.

Sicherheit ist eingebaut

Darauf kannst du dich verlassen

- **Standardmäßig nur lesend.** Scan, Karte, Abgleich, Debugger und Bericht ändern nichts.
- **Jede Änderung mit Vorschau und Bestätigung,** auf der Kommandozeile nur mit „--ausfuehren“. Vorher wird die komplette Firewall-Konfiguration gesichert, jede Änderung steht im Änderungsprotokoll.
- **Niemand sperrt sich aus:** Pflichtregeln für das Admin-Netz, Abbruch bei einer RDP-Sitzung von außerhalb, Totmannschalter mit automatischer Rückkehr.
- **Gruppenrichtlinien werden respektiert** und lokal nicht übersteuert. GPOs legt das Werkzeug nur auf ausdrücklichen Wunsch an, mit Vorschau und vorheriger Sicherung.
- **Erfolg nur nach dem Zurücklesen:** Ein „erledigt“ gibt es erst, wenn die Werte nachweislich dort stehen, wo sie hingehören.
- **Ehrliche Bewertung:** Was nicht sicher bestimmbar ist, heißt „unklar“ und wird nicht schöngerechnet.
- **Alles bleibt im Haus:** keine Telemetrie, keine Online-Aufrufe, keine Updateprüfung, kein Installer, keine Registrierungseinträge.
- **Signierte EXE** mit Prüfsummen zu jeder Version.

Bericht, Kommandozeile und Sammelbetrieb

Bericht mit Firewall-Ausnahmenregister

Der Bericht als Word, PDF, CSV oder JSON ist um das Firewall-Ausnahmenregister herum aufgebaut: jede Freigabe mit Anwendung, Ports, Quelle, Herkunft, Wirksamkeit, Begründung, verantwortlicher Person und Ablaufdatum. Was du bewusst nicht freigegeben hast, steht mit Begründung in einem eigenen Abschnitt. Das ist der Nachweis für Audit, Datenschutz und Leitung. Einen anonymisierten Musterbericht mit fiktiven Daten findest du im Download-Bereich.

Kommandozeile

Oberfläche und Kommandozeile stecken in derselben EXE. Ohne Argumente startet die Oberfläche, mit Argumenten der Konsolenmodus mit sprechenden Exit-Codes für Skripte, geplante Aufgaben und Softwareverteilung.

Befehl	Was er tut	Ändert etwas?
scan	Ports, Prozesse und Firewall erfassen und bewerten; Ausgabe als JSON, Word, PDF, CSV	nein
bericht	Bericht aus einer vorhandenen Scan-Datei	nein
sammeln	Sammelbericht über viele Scans mit gemeinsamer Regelbasis als GPO-Skript	nein
regel-pruefen	Regel-Debugger: Wird Quelle X auf Port Y zugelassen?	nein
geblockt	verworfene Verbindungen je Port und Quellnetz	nein
vorschlaege	Regelvorschläge aus dem Lernprotokoll	nein
lernmodus	Lernmodus starten, prüfen, beenden, Protokoll verdichten	start/ende: ja

Befehl	Was er tut	Ändert etwas?
testregeln	Testregeln anzeigen oder entfernen	entfernen: ja
scharfschalten	Pflichtregeln, freigegebene Regeln, „Blockieren“, Totmannschalter	ja
bestaetigen / rueckgaengig	Scharfschaltung bestätigen bzw. Sicherung wiederherstellen	ja

Sammelbetrieb

Für viele Maschinen läuft der Scan als Startskript, geplante Aufgabe, per PsExec oder als Intune-Skript. Jede Maschine schreibt ihre Datei auf eine Freigabe, der Sammelbericht fasst alles zusammen: Lücken und Herkunft über alle Maschinen, dazu eine gemeinsame Regelbasis als GPO-Skript.

```
WinFirewallDiagnostiker.exe scan --ausgabe \\fs01\WfdScans$ --still
WinFirewallDiagnostiker.exe sammeln --ordner \\fs01\WfdScans$ --ausgabe C:\Berichte
```

Kostenlos oder Pro: die Editionen im Vergleich

Der Grundsatz: **Kostenlos ist alles, was eine einzelne Maschine sicher macht. Die Pro-Edition ist für alle, die ganze Flotten einschalten, Regelwerke für viele Rollen bauen oder von der GPO nach Intune umziehen.** Die kostenlose Edition ist dabei keine Demo: Mit ihr kannst du eine Maschine vollständig analysieren, im Lernmodus beobachten, testen und scharf schalten.

Funktion	Kostenlos	Pro
Analyse einer Maschine		
Lagebild, Anwendungskarte, Lückenliste, Regel-Debugger	ja	ja
Abgleich zentral gegen tatsächlich (GPO und Intune)	ja	ja
Bericht mit Firewall-Ausnahmenregister (Word, PDF, CSV, JSON)	ja	ja
Einschalten einer Maschine		
Lernmodus-Assistent für lokalen Weg, GPO-Weg und Intune-Weg	ja	ja
Testregeln mit Ablaufzeit, Planungskorb, GPO-Skript	ja	ja
Scharfschalten mit Totmannschalter, Auswertung geblockter Verbindungen	ja	ja
Viele Maschinen		
Sammelbetrieb per Kommandozeile, Sammelbericht mit gemeinsamer Regelbasis	ja	ja
Lernmodus per GPO für viele Maschinen, Lernzeitraum im Sammelbericht	ab Version 2.1	ab Version 2.1
Export als Intune-Richtlinie, Gegenprobe, Scan-Vergleich	ab Version 2.1	ab Version 2.1
Zentrale Auswertung mit individuellen Regelsätzen je Maschine	–	ja
GPO-Designer: Rollen erkennen, Basis- und Rollen-GPOs vorschlagen, Wirkung simulieren	–	ja
Einführung in Ringen planen und verfolgen	–	ja

Funktion	Kostenlos	Pro
Betrieb und Intune		
Migrationsassistent: Firewall-Regeln von der GPO nach Intune	–	ja
Drift-Überwachung mit Meldung bei neuen Ports und verschwundenen Regeln	–	ja
Nachweisberichte für Audit und Leitung über alle Maschinen	–	ja
Lizenz		
Preis	kostenlos	auf Anfrage
Verfügbarkeit	jetzt	in Vorbereitung, Pilotkunden willkommen

Wann sich Pro lohnt

- Du willst die Firewall nicht auf einer, sondern auf Dutzenden oder Hunderten Maschinen einschalten.
- Du brauchst ein Regelwerk aus Basis- und Rollen-GPOs statt Einzelregeln je Maschine.
- Du ziehst von Gruppenrichtlinien nach Intune um und willst das Regelwerk dabei mitnehmen.
- Du musst gegenüber Audit, Datenschutz oder Leitung regelmäßig nachweisen, dass das Regelwerk stimmt.

Pilotkunde werden

Die Pro-Edition entsteht gerade, und zwar mit echten Umgebungen im Blick. Wenn du ein konkretes Vorhaben hast, etwa eine Domäne mit abgeschalteter Firewall oder einen Umzug nach Intune, melde dich. Pilotkunden bekommen die Pro-Funktionen früh und reden bei den Details mit.

Beratung: „Windows-Firewall einschalten“ als Projekt

Das Werkzeug macht das Einschalten beherrschbar. Die Entscheidungen bleiben trotzdem bei dir: Welche Fachanwendung braucht was, welche Rollen gibt es, wer gibt eine Ausnahme frei, und wie wird das Regelwerk gepflegt, wenn die nächste Software kommt?

Was ich als Projekt anbiete

- **Bestandsaufnahme** mit Sammelbericht und einer ehrlichen Einschätzung, wo es wehtun wird.
- **Lernphase** in einer Pilotgruppe, mit sauber gebauter Lern-GPO.
- **Regelwerk** mit deinen Fachabteilungen und Herstellern, als Basis- und Rollen-GPOs oder gleich in Intune.
- **Scharfschalten in Ringen** mit Rückweg in jeder Phase.
- **Übergabe** mit Ausnahmenregister und Pflegeprozess, damit das Regelwerk nicht wieder verwildert.

Technische Daten

Merkmal	Angabe
Betriebssysteme	Windows 10 und 11, Windows Server 2016 und neuer
Architektur	x64 und ARM64, je eine eigene EXE
Lieferform	eine signierte EXE, keine Installation, keine .NET-Installation nötig; Prüfsummen in SHA256SUMS.txt
Bedienung	Oberfläche und Kommandozeile in derselben Datei
Rechte	Administrator empfohlen; ohne Adminrechte läuft das Werkzeug, kennzeichnet das Ergebnis aber als unvollständig und sperrt ändernde Aktionen
Steuerung der Firewall	lokal, gemischt, Gruppenrichtlinie oder Intune, automatisch erkannt
Ausgaben	Word, PDF, CSV, JSON; PowerShell-Skripte für die GPO-Verwaltung
Dateiablage	nur im gewählten Ausgabeordner und, bei ändernden Aktionen, im Arbeitsordner unter %ProgramData%
Datenschutz	keine Telemetrie, keine Online-Aufrufe, alle Daten bleiben auf der Maschine
Sprache	Deutsch
Aktuelle Version	2.0.1

Häufige Fragen

Ändert das Werkzeug etwas, wenn ich es einfach starte?

Nein. Scan, Anwendungskarte, Abgleich, Debugger und Bericht sind ausschließlich lesend. Ändernd sind nur Lernmodus, Testregeln, Anwenden aus dem Planungskorb, Scharfschalten und Rückgängig, und jede dieser Aktionen zeigt vorher alle Schritte und braucht deine Bestätigung.

Muss ich es auf jeder Maschine einzeln ausführen?

Für die Analyse einer einzelnen Maschine ja, denn nur dort sind Prozesse und Ports sichtbar. Für viele Maschinen gibt es den Sammelbetrieb: Scan per Startskript, geplanter Aufgabe oder Intune-Skript, Ergebnisse auf eine Freigabe, daraus ein Sammelbericht.

Unsere Firewall ist per GPO abgeschaltet. Reicht es, die GPO zu entfernen?

Technisch ja, praktisch ist das der riskanteste Weg. Ohne GPO gilt die lokale Einstellung, und die steht ab Werk auf „Ein“ mit „eingehend blockieren“. Alle betroffenen Maschinen schalten beim nächsten Richtlinienabgleich gleichzeitig scharf. Sicherer ist eine Lern-GPO mit höherer Rangfolge für eine Pilotgruppe, wie im Abschnitt „Praxis“ beschrieben.

Kann ich lokale Testregeln anlegen, obwohl die Firewall zentral gesteuert wird?

Ja, sofern „Lokale Firewallregeln anwenden“ in der GPO bzw. in Intune nicht auf „Nein“ steht. Die Profileinstellungen wie der Firewallstatus kommen aber weiter aus der zentralen Vorgabe. Ist die Firewall dort aus, wirken auch lokale Regeln nicht.

Wie lange sollte der Lernmodus laufen?

So lange, bis die Abdeckungskurve flach ist, also keine neuen Zugriffe mehr auftauchen. Mit Monatsabschluss, Backup-Läufen und Patchday sind das in der Praxis rund vier Wochen.

Funktioniert das auch mit Intune?

Ja. Das Werkzeug erkennt Regeln und Einstellungen aus Intune, zeigt ihre Herkunft und warnt bei Mischbetrieb mit GPOs. Der Lernmodus-Assistent nennt für den Intune-Weg die nötigen Einstellungen. Der Export als Intune-Richtlinie folgt mit Version 2.1.

Was ist mit Store-Apps wie Teams?

Regeln von Store-Apps gelten nur für ihr App-Paket, auch wenn sie weder Programm noch Port nennen. Das Werkzeug wertet diesen Paketbezug aus. Eine solche Regel deckt also nicht versehentlich einen Dienst ab, der zufällig auf demselben Port lauscht.

Was kostet die Pro-Edition?

Die Pro-Edition ist in Vorbereitung; Lizenzmodell und Preis stehen noch nicht fest. Die kostenlose Edition bleibt kostenlos, auch wenn Pro erscheint. Wer Interesse an Pro hat, kann sich als Pilotkunde melden.

Brauche ich eine Internetverbindung oder ein Konto?

Nein. Keine Registrierung, keine Lizenzprüfung für die kostenlose Edition, keine Telemetrie, keine Online-Aufrufe.

Download und Kontakt

Download der aktuellen Version mit Prüfsummen und anonymisiertem Musterbericht: https://ubb-downloads.azurewebsites.net/

Fragen, Pilotprojekt oder Beratung: **Ulrich B. Boddenberg**, IT-Consulting · Software Engineering · Technologieseminare, Dortmund.

E-Mail: ulrich@boddenberg.de

Web: https://www.boddenberg.de/