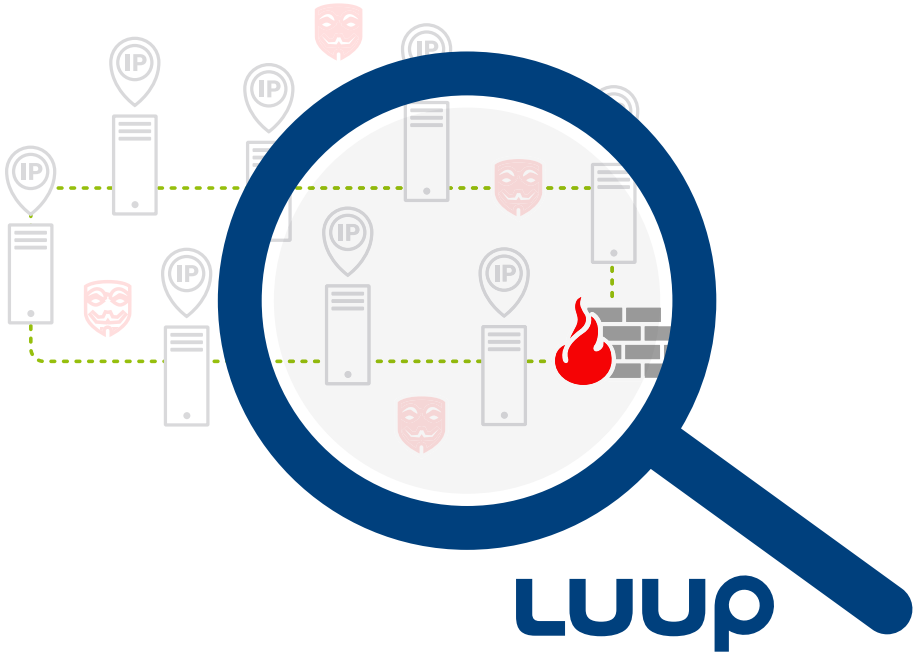
Luup

SecurITy made in Germany

**WHITEPAPER**

Best Practice

# Firewall Management-Monitoring




Luup unterstützt Sie bei Ihren

## Compliance-Anforderungen

- BSI Grundschutz
- ISO 27001
- PCI/DSS
- DSGVO

## EINLEITUNG

*„Eine Firewall sollte von jedem Unternehmen als minimale Schutzmaßnahme vor Bedrohungen aus dem Internet eingesetzt werden.“*

**Mit dieser einmaligen Einrichtung ist es allerdings nicht getan.**
Noch immer erfolgt die Pflege der sogenannten Firewallregeln oder Firewallpolicy in vielen Unternehmen lediglich auf Zuruf.

Auch regelmäßige Updates von Firewalls werden eher selten durchgeführt, da diese durch die verursachten Unterbrechungen der Verbindungen zu Verzögerungen oder Ausfällen im Arbeitsablauf führen können.

## DAS MOTTO FÜR ANPASSUNGEN

Wenn die für den neuen Businessprozess dringend erforderliche Firewall-Änderung erfolgt ist und keine Auffälligkeiten auftreten, ist „gefühlt“ alles in Ordnung.

Änderungen müssen immer häufiger unter Zeitdruck vorgenommen werden – danach bleibt keine Zeit für Reviews oder Qualitätskontrolle.

*“Wir brauchen die Verbindung zum ERP-System bis heute abend, damit wir die Geschäftszahlen reporten können. Machen Sie im Zweifel einfach alles auf, wir können das ja in den nächsten Tagen einschränken.”*

*“Ja, das System ist ausgebaut, den Rest machen wir später / Die Firewallpolicy können wir später bereinigen.”*

*“Wir deployen das neue Testsystem im gleichen Netzsegment wie die Produktion. Das Testsystem muss Herr Meyer auf Port 23 erreichen können. Die Policy bereinigen wir, wenn wir das Testsystem in die Produktion überführen.”*

## FIREWALL-MANAGEMENT IN 6 SCHRITTEN.

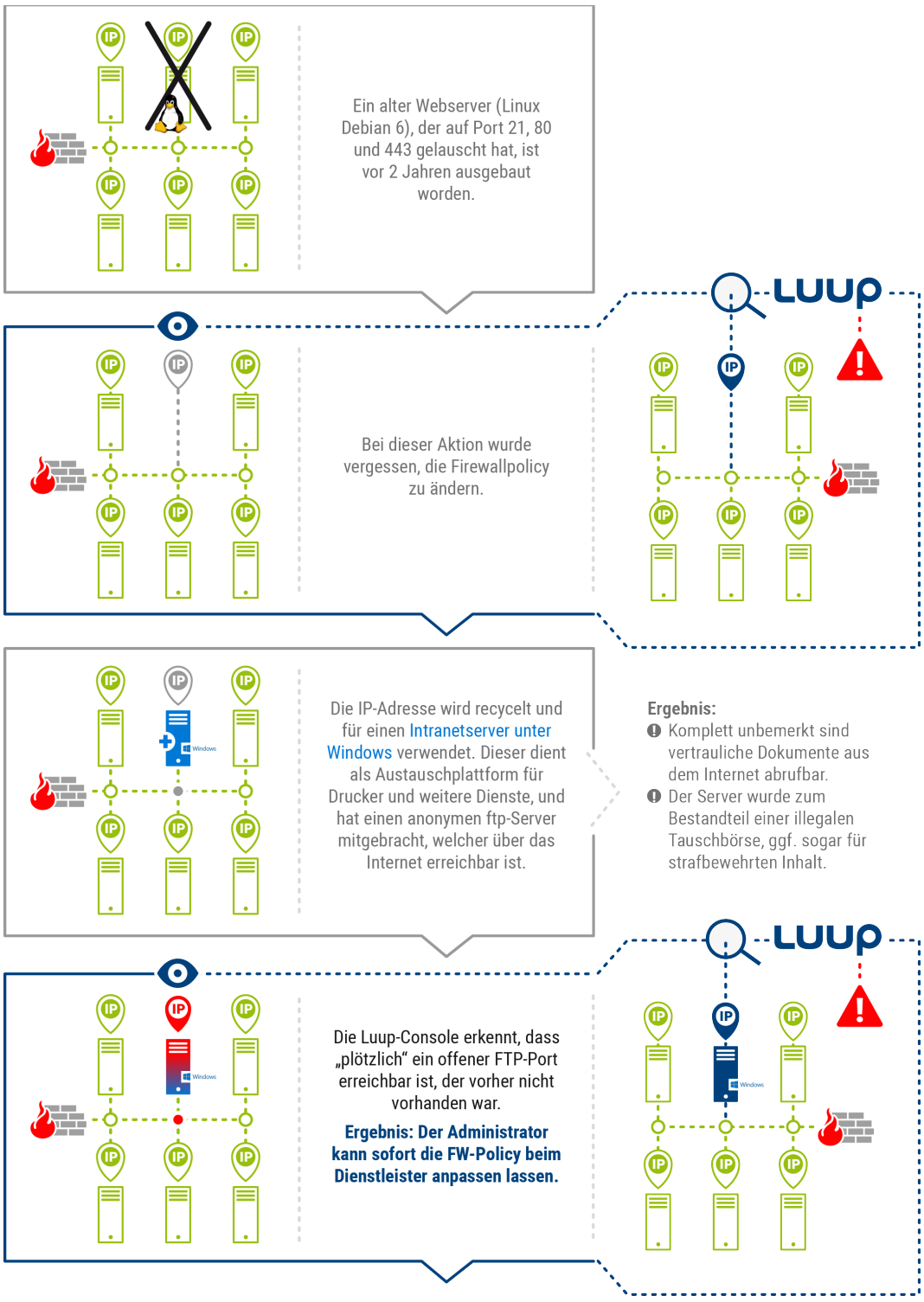
**EIn gutes Firewall-Management sollte Planungs- und Verifikationsschritte beinhalten. Zudem ist eine regelmäßige und unabhängige Qualitätskontrolle unabdingbar.**

1. Ist eine Änderung wirklich erforderlich und passt sie zum Sicherheitskonzept?
2. Änderungen planen / Planung dokumentieren.
3. **Change veranlassen und bei größeren Änderungen eine Kontrollinstanz zur Überprüfung einsetzen.**
4. Automatische Sicherung der Konfiguration durchführen, um Änderungen erkennbar und nachvollziehbar zu machen.
5. **Nach den Änderungen prüfen, ob es Seiteneffekte gibt.**
6. **Regelmäßig automatisch von extern prüfen (lassen), ob ungewollte IP-Adressen und/oder Ports erreicht werden können.**

Erklärung: **Luup** hilft bei den Schritten 3, 5 und 6 (s. nachfolgende Seite)

## FIREWALL-MANAGEMENT MIT **Luup** – EIN BEISPIEL:

Vor
2 Jahren



## ÜBER Luup

Die automatische Kontrolle mit einer Risikobewertung informiert sowohl Technik als auch Management über neue IP/Ports bzw. Änderungen. Alle daraus gewonnenen Daten und Informationen werden zusammengeführt und in einer kompakten Ansicht dargestellt.
Auf diese Weise findet zum einen komplett automatisiert eine unabhängige Qualitätssicherung Ihrer Infrastruktur statt – **zum anderen kann so gesehen werden, was der oder ein Angreifer sieht!**

Auf Anfrage besteht weiterhin die Möglichkeit, Daten für Compliance-Nachweise oder eine konkrete Tiefenanalyse zu erhalten.

**Auf einen Blick: Ihre Vorteile für die Arbeit mit Luup**

- **Wichtige Informationen für die Netzhygiene (Reverse Lookups, SSL-Zertifikate);**
- **Qualitätssicherung für Managed Firewall;**
- **Sicht auf die Schatten-IT;**
- **Eine bewertete Liste ermöglicht auch Leitungskräften den Überblick zu gewinnen;**
- **Material für Notfallmanagement: welche Systemen stehen mir zur Verfügung?**
- **Luup unterstützt Sie bei Ihren Compliance-Anforderungen (BSI Grundschutz, ISO 27001, PCI/DSS, DS- GVO).**