SOPHOS XG FIREWALL ERSTEINRICHTUNGSANLEITUNG

STANDARDKONFIGURATION NACH BEST PRACTICE

ADRIAN PAWLICZUK
IDERI GMBH
Info@ideri.com
+49 159 02609288

Dokumentart:	Technische Anleitung
Version:	11.1
Gültig für:	Sophos XG Firewall v18.x
Erstellung:	2023
Stand	07/2025

1 Einleitung

Herzlichen Glückwunsch zur Entscheidung für eine Sophos XGS Firewall – dem Herzstück Ihrer IT-Sicherheitsstrategie! Eine optimal konfigurierte Firewall ist von entscheidender Bedeutung, um Ihr Unternehmen effektiv vor Cyber-Bedrohungen, Datenverlusten, unerlaubten Zugriffen und kostspieligen Betriebsunterbrechungen zu schützen. Gerade in Zeiten zunehmender digitaler Vernetzung und stetig wachsender Cyberrisiken stellt eine robuste Firewall-Lösung das zentrale Element Ihrer Sicherheitsarchitektur dar.

Die Ersteinrichtung einer Firewall wie der Sophos XGS kann jedoch komplex und zeitaufwendig sein. Fehler in der Konfiguration können gravierende Sicherheitsrisiken nach sich ziehen, weshalb eine sorgfältige und professionelle Erstinstallation unerlässlich ist. Es geht nicht nur darum, grundlegende Sicherheitsstandards zu erfüllen – Ihre Firewall sollte auch maßgeschneidert auf die individuellen Anforderungen und Geschäftsprozesse Ihres Unternehmens abgestimmt sein.
Genau hier kommt die IDERI GmbH als erfahrener Managed Service Provider ins Spiel. Seit vielen Jahren unterstützen wir kleine und mittelständische Unternehmen dabei, ihre IT-Infrastruktur professionell abzusichern und durch fortlaufende Betreuung dauerhaft sicher zu halten. Unsere spezialisierten Experten kümmern sich umfassend um Ihre Sophos XGS Firewall und sorgen dafür, dass Sie jederzeit optimal geschützt sind.

Mit unserem Managed Firewall Service bieten wir Ihnen eine professionelle Sicherheitslösung zum monatlichen Festpreis, die weit über die einfache Bereitstellung der Hardware hinausgeht. Zu unseren umfangreichen Leistungen gehören:

- **Komplettes Management Ihrer Firewall per Fernwartung**: Sie brauchen sich um nichts zu kümmern – unser Team übernimmt die gesamte technische Betreuung.
- **Regelmäßige Sicherheitsupdates**: Wir sorgen dafür, dass Ihre Firewall stets mit den neuesten Firmware-Updates versorgt wird, um optimal gegen aktuelle Bedrohungen geschützt zu sein.
- **Individuelle Konfiguration nach Ihren Anforderungen**: Unsere Spezialisten passen Ihre Firewall exakt auf die Bedürfnisse Ihres Unternehmens an. Dazu zählen auch spezifische Sicherheitsregeln, die beispielsweise den Zugriff auf bestimmte Webseiten oder Dienste einschränken können.
- **Einrichtung sicherer Zugänge**: Wir konfigurieren abgesicherte Zugänge für Ihre Mitarbeiter im Home-Office und Außendienst – für maximale Flexibilität ohne Kompromisse bei der Sicherheit.
- **Kontinuierliches Monitoring und proaktive Wartung**: Angriffsversuche, Sicherheitsprobleme und sonstige Unregelmäßigkeiten werden automatisch erkannt und direkt an unsere Techniker gemeldet, die unverzüglich reagieren können.
- **Transparente Berichterstattung**: Sie erhalten regelmäßige Berichte zur Sicherheitslage Ihrer IT, damit Sie jederzeit informiert sind.

Für eine optimale Sicherheit empfehlen wir, die Erstkonfiguration Ihrer Sophos XGS Firewall direkt von unseren Experten durchführen zu lassen. Diese übernehmen dabei nicht nur die grundlegende Installation, sondern berücksichtigen auch spezifische Anforderungen und Wünsche Ihres Unternehmens. So stellen wir sicher, dass Ihre Firewall genau die Sicherheitslevel bietet, die Sie wirklich benötigen.

Bitte beachten Sie, dass sich diese Anleitung auf die Firmware Version 18 bezieht. Aufgrund der hohen Dynamik im Bereich der IT-Sicherheit können wir diese Dokumentation leider nicht bei jeder Aktualisierung der Firmware erneuern. Mit unserem Managed Firewall Service sind Sie jedoch stets auf der sicheren Seite – wir behalten für Sie stets den Überblick und sorgen dafür, dass Ihre Firewall kontinuierlich auf dem neuesten Stand ist.
Setzen Sie auf IDERI für maximale IT-Sicherheit, minimalen Aufwand und absolute Planungssicherheit – damit Sie sich voll und ganz auf Ihr Kerngeschäft konzentrieren können.

Inhaltsverzeichnis

2 Zweck und Geltungsbereich

Diese Anleitung bietet eine umfassende Handreichung für die Inbetriebnahme und Einrichtung von Sophos XG Firewalls nach bewährten Sicherheitsstandards. Das Dokument enthält grundlegende Konfigurationsanweisungen für verschiedene Einrichtungsstadien einer Sophos XG Firewall und bildet den Rahmen für eine vollständige Sophos XG-Konfiguration.

> **Wichtiger Hinweis:** Es ist essentiell, während der Konfiguration auf individuelle Kundenanforderungen einzugehen und entsprechende Anpassungen durchzuführen. Eine 1:1-Übernahme der Konfiguration auf jede Umgebung ist weder möglich noch empfehlenswert.

Zielgruppe: Diese Anleitung richtet sich an Systemadministratoren und Techniker, die mit den Funktionen einer Next Generation Firewall vertraut sind.

3 Allgemeine Einrichtung

3.1 Registrierung und Lizenzierung

Die Registrierung erfolgt über einen Sophos-ID Account (https://id.sophos.com). Falls noch kein Account vorhanden ist, muss ein neuer erstellt und die Lizenzen dort aktiviert werden.

Für den Konfigurationszeitraum vor der Produktivstellung kann eine Registrierung über die 30-Tage-Testversion erfolgen. Mit der Übergabe wird die entsprechend erworbene Subscription freigeschaltet.

3.2 Admin und User Settings

Der Zugriff auf die Admin-Konsole sollte auf den FQDN der Firewall konfiguriert werden. Dies ermöglicht bei Bedarf auch externe Zugriffe (z.B. auf das User Portal) über den konfigurierten FQDN. Hierfür ist die Einrichtung eines A-Records auf die öffentliche IP-Adresse der Firewall erforderlich.

Externe Konfiguration: Entsprechendes Zertifikat auswählen

Falls der externe Zugriff nicht gewünscht ist, sollte die Option "Use a different hostname" ausgewählt werden.

> **Konvention für internen FQDN:** portal.domaene-intern.local

3.3 Externe Administration

Die Verwaltung der Firewall sollte grundsätzlich nur intern möglich sein (Standardeinstellung). Für die Ersteinrichtung kann eine Freischaltung des WAN-Zugriffs über Administration → Device Access erfolgen. Vor der Produktivstellung ist der Zugriff wieder zu deaktivieren.

Die empfohlene Best Practice für die Firewall-Administration stellt der Zugriff über das Sophos Central Portal dar (siehe Kapitel 16: Central Synchronisation).

3.4 Device Access

3.4.1 Login Security

Die Login Security muss aktiviert werden. Diese blockiert ungültige Anmeldeversuche nach 5 Versuchen für 60 Sekunden.

3.4.2 Passwort-Komplexität

Die Komplexitätsanforderungen für das Administrator-Kennwort müssen aktiviert werden.

> **Wichtiger Hinweis:** Die Verwendung eines Ausrufezeichens als Symbol ist entgegen der Sophos-Dokumentation nicht zulässig.

4 Gerätekonfiguration

4.1 LAN-Bridge Konfiguration

Bei kleineren Hardware-Appliances ist oft eine vordefinierte LAN-Bridge vorhanden, die mehrere LAN-Ports zusammenfasst. Diese Bridge-Konfiguration muss aufgelöst werden, da sie häufig zu Problemen führt.

4.2 NTP-Server

Für die Zeitsynchronisation sollte NTP aktiviert werden. Verwenden Sie immer die "predefined NTP Server" der Sophos Appliance.

Da die Sophos XG keinen eigenen NTP-Server mehr bereitstellt, kann über die NAT-Engine eine NTP-Proxy-ähnliche Funktionalität erreicht werden. Dadurch kann NTP-Verkehr transparent an einen internen oder externen NTP-Server weitergeleitet werden.

4.3 E-Mail-Benachrichtigungen

Es sollte nach Möglichkeit immer ein externer Mailserver konfiguriert werden.

Nach erfolgreichem Test der E-Mail-Benachrichtigung müssen die Einstellungen des automatischen Backups überprüft und gegebenenfalls angepasst werden. Empfohlen wird ein wöchentliches Backup der Konfiguration. Das Encryption Password und der Storage Master Key müssen dokumentiert werden, damit bei Hardware-Defekten ein Backup zur Wiederherstellung der Einstellungen genutzt werden kann.

Best Practice ist der automatische Transfer des Backups an das Sophos Central Dashboard.

5 Authentifizierung

5.1 AD-Authentifizierung einrichten

Um Active Directory Sicherheitsgruppen nutzen zu können, muss eine Verbindung zu allen Domain Controllern eingerichtet werden. Für die Verbindung wird ein AD-Benutzerkonto ohne besondere Rechte benötigt.

> **Wichtig:** Es ist ausschließlich LDAPS zulässig. (LDAPS-Abfragen funktionieren nur, wenn eine Certificate Authority auf dem Domain Controller installiert ist)

5.2 Import von Sicherheitsgruppen

Nach der erfolgreichen Verbindung zum Active Directory können über die entsprechende Schaltfläche Sicherheitsgruppen importiert werden.

5.3 Authentifizierungsdienste

Hier wird festgelegt, wer sich für welchen Dienst authentifizieren darf. Diese Einstellungen müssen entsprechend der Umgebung angepasst werden. Soll beispielsweise SSL VPN mit AD-Anmeldung genutzt werden, muss dies an den entsprechenden Stellen aktiviert werden.

6 SIP Helper Deaktivierung

In den meisten Installationen, bei denen SIP genutzt wird, kann der SIP Helper gemäß der Sophos Knowledge Base (KB-000035917) deaktiviert werden. In seltenen Fällen wird er jedoch benötigt. Standardmäßig sollte dieser deaktiviert werden.

7 Firewall-Konfiguration

7.1 Policy Settings

7.2 Gruppierung

Für eine bessere Übersicht im Regelwerk sollten die Policies gruppiert werden. Folgende Gruppierungen werden empfohlen:

- **.LAN-to-WAN** - LAN-Kommunikation zum Internet
- **.DMZ-to-WAN** - DMZ-Kommunikation zum Internet
- **.WiFi-to-WAN** - WLAN-Kommunikation zum Internet
- **.WAN-to-DMZ** - Externe Zugriffe auf DMZ-Ressourcen

Es sollten nicht für jeden Dienst separate Regeln erstellt werden, sondern die Dienste sinnvoll in den Regeln zusammengefasst werden. Je mehr Regeln angelegt sind, desto mehr Performance benötigt die XG.

Der vorangestellte Punkt kennzeichnet manuell angelegte Regeln. Die automatische Gruppierung kann genutzt werden, führt aber in komplexen Umgebungen gelegentlich zu Fehlern.

7.2.1 Wichtige Firewall-Regeln

Es ist zwingend erforderlich, die Regel "Any Deny" anzulegen und diese ohne Gruppierung an die unterste Position zu setzen. Seit Version 18 ist die ANY DENY-Regel Standard. Mit der Neuanlage eines Clones wird lediglich die Firewall-Protokollierung aktiviert.

> **Wichtiger Hinweis:** Es ist untersagt, als Quell- und Zielzone "Any" auszuwählen. Alle Zonen müssen manuell ausgewählt werden.

In Verbindung mit Sophos Central und Synchronized Security muss DNS vom Domain Controller ins WAN und von den entsprechenden Clients zum Domain Controller ohne Heartbeat-Auswertung in eigenen Regeln freigegeben werden.

> **Empfohlene Gruppierung:** .DNS-to-WAN - Domain Controller zu WAN

7.2.2 Benutzerdefinierte Objekte

Für gezielte Freigaben für bestimmte Hosts, Netzwerke oder Dienste können benutzerdefinierte Objekte angelegt werden. Zur besseren Identifikation sollte eine spezielle Benennung verwendet werden:

- **.H_Servername** - Hostobjekt für einen Server (z.B. 192.168.1.1)
- **.N_Produktion** - Netzwerkobjekt für ein IP-Segment (z.B. 192.168.1.0/255.255.255.0)
- **.S_HBCI_3000** - Serviceobjekt für einen Dienst (z.B. 3000/TCP)

So ist die Einstellung der Firewall-Regel bereits anhand der genutzten Objekte erkennbar.

7.2.3 Security Features

Grundsätzlich sollte auf allen Regeln das Logging aktiviert werden. Sofern in der Subscription enthalten, sollte auch Sandstorm aktiviert werden. Des Weiteren sollten auch der Virenscanner und IPS immer aktiv sein, mindestens jedoch auf allen Regeln, die nach extern kommunizieren.

7.2.4 SSL/TLS-Entschlüsselung – DPI-Engine / Web-Proxy

Da über 80% des Datenverkehrs mittlerweile SSL-Traffic ist, sollten Schadprogramm- und Inhaltsscans sowie SSL Traffic Scanning via DPI-Engine oder Web-Proxy durchgeführt werden.

HTTP-Traffic kann die Firewall problemlos prüfen, da dieser unverschlüsselt ist. HTTPS-Traffic muss hingegen zuerst entschlüsselt werden. Das Problem war bisher, dass der Web-Proxy nur HTTPS-Traffic über Port 443 entschlüsseln konnte. Traffic über andere Ports (z.B. https://www.example.com:8000) konnte nicht geprüft werden.

Mit Version 18 kann sowohl SSL- als auch TLS 1.3-Traffic geprüft werden, unabhängig von Ports oder Protokollen.

Die Sophos Firewall bringt ein neues DPI-Modul mit, um Internetverkehr transparent zu filtern und verschlüsselten Verkehr zu inspizieren. Es bietet die beste Leistung bei Webfilter, Inhaltsscannung und SSL/TLS-Inspektion und ist unter Firewall → SSL/TLS-Inspektionsregeln standardmäßig aktiviert.

Der Web-Proxy ist als Alternative weiterhin verfügbar. Es gibt wenige Gründe, nicht auf die neue DPI-Engine zu setzen. Dennoch bietet der Web-Proxy Funktionen, die die DPI-Engine nicht hat, wie SafeSearch für Suchmaschinen oder YouTube, Caching oder Pharming Protection.

Bei der Aktualisierung von Version 17.5 auf 18.0 werden die Web-Proxy-Einstellungen übernommen. Für die Nutzung der DPI-Engine muss eine SSL/TLS-Inspection-Regel angelegt und der Web-Proxy in den Firewall-Einstellungen deaktiviert werden.

> **Wichtiger Hinweis:** Es werden erst die Firewall-Regeln, dann die SSL/TLS-Inspektionsregeln und anschließend die Webfilterregeln abgearbeitet. Für das Scannen von SSL/TLS-Verbindungen auf allen Ports über gesamte Zonen und Netzwerke müssen entsprechende SSL/TLS-Verbindungsregeln angelegt werden.

7.2.5 Weitere Einstellungen:

- **QUIC-Protokoll aktivieren:** Websites wie Google, die QUIC verwenden, können Webfilterung umgehen. Das Aktivieren dieser Option stellt sicher, dass diese Seiten HTTP/S verwenden.
- **Zero-Day-Schutz:** Bei gültiger Sandstorm-Subscription unbedingt aktivieren.
- **FTP auf Schadprogramm scannen:** Die meisten FTP-Anwendungen haben Probleme mit der Aktivierung dieser Funktion.

Wenn eine gültige Subscription für Web Protection vorhanden ist, sollte vor der Implementierung auf die Vorteile des HTTPS Traffic Scans hingewiesen werden.

Da beim Entschlüsseln des HTTPS-Traffics ein Eingriff in den Datenverkehr stattfindet, muss dieser mit einem gültigen Zertifikat autorisiert werden:

- Root-CA-Zertifikat der internen Stammzertifizierungsstelle wird in Sophos XG hinzugefügt
- oder SecurityApplianceCA.pem der Sophos XG wird an Endpoints verteilt (auch über GPO möglich)

> **Fehlerpotentiale beachten:**

- Nur IE/Edge/Chrome/Mozilla greifen auf den gemeinsamen Zertifikatspeicher zu
- Anwendungen, die via SSL kommunizieren und nicht auf den internen Zertifikatspeicher zugreifen, benötigen URL-basierte Ausschlüsse
- Updates können Anpassungen in der Firewall erfordern

Empfehlung: Einrichtung der DPI-Engine / SSL-Scan & Decrypt. Der administrative Aufwand im Nachgang ist erhöht und muss bewusst sein.

7.2.6 Synchronized Security Heartbeat

Bei der Nutzung von Sophos Endpoint-Virenscanner und Sophos Central darf die Einstellung für Synchronized Security Heartbeat nicht auf "GREEN" eingestellt werden. Wenn Clients einen ausstehenden Neustart haben, führt das zum Status "YELLOW". Daher die Einstellung maximal auf "YELLOW" erhöhen.

Richtlinien für die DNS-Auflösung von Clients zu Servern immer auf "No Restriction" belassen. Auch der DNS-Server/Domain Controller sollte immer per DNS kommunizieren können. Management-Server sollten keine Heartbeat-Auswertung erfahren, um Remotezugriff zu ermöglichen.

Anwendung: Dies findet nur Anwendung auf .DNS-To-WAN!

8 Routing-Einstellungen

8.1 SD-WAN Routing

Für die Bindung bestimmten ausgehenden Datenverkehrs an eine WAN-Schnittstelle muss eine SD-WAN-Policy erstellt werden. Diese kann auf einzelne Dienste, Hosts oder ganze Netze angewendet werden.

Standardmäßig arbeitet die Sophos XG(S) Firewall erst SD-WAN-Policies, dann VPN-Routen und anschließend statische Routen ab. Beim Einsatz von SD-WAN-Policies kann es zu Routing-Problemen kommen. Es wird empfohlen, die Reihenfolge über das CLI zu ändern:

1. Verbindung über Shell (SSH)
2. Device Console öffnen
3. Reihenfolge prüfen: `system route_precedence show`
4. Befehl eingeben: `system route_precedence set static vpn sdwan_policyroute`
5. Reihenfolge erneut prüfen: `system route_precedence show`

9 Web-Konfiguration

9.1 Office/Microsoft 365 FQDN Import

Für die Nutzung von Office/Microsoft 365 sollte eine Liste mit FQDNs und IP-Netzwerken importiert werden. Wählen Sie bei den zu importierenden Exclusions zwischen:

- API-O365-all.tar
- API-O365-minimal.tar
- API-O365-required.tar

Dies fügt eine Gruppe von Ausnahmen hinzu, die für die Nutzung von Office/Microsoft 365 erforderlich ist.

10 Web Application Firewall

Eine externe Veröffentlichung von Webservern ist ausschließlich über die WAF durchzuführen. Der Webserver darf nicht per D-NAT veröffentlicht werden, es sei denn, die notwendige Lizenz wurde nicht erworben und über das Sicherheitsrisiko wurde schriftlich informiert.

10.1 Webfilter-Richtlinien und Ausnahmen

Bei der Definition von Webfilter-Ausnahmen werden nur wirklich relevante, minimal notwendige Freigaben importiert.

10.2 Webfilter-Richtlinien für Microsoft Exchange Server

10.2.1 WAF-Richtlinie Autodiscover

Diese Richtlinie ist standardmäßig vorkonfiguriert und muss nur überprüft werden. Beachten Sie die Infrastructure-Policies der WAF ModSecurity in Zusammenhang mit dem Versionsstand der Firewall.

> **Wichtiger Hinweis:** Infrastrukturregeln sind der Kern des WAF ModSecurity-Betriebs. Diese Regeln sollten nicht deaktiviert werden, da andere Regeln darauf aufbauen können. Das Hinzufügen einer Infrastrukturregel zur Liste "Filterregeln überspringen" kann andere Angriffe ermöglichen.

10.2.2 WAF-Richtlinie Exchange General

Diese Richtlinie ist standardmäßig vorkonfiguriert und muss bearbeitet werden. Je nach Umgebung müssen die entsprechenden Pfade konfiguriert werden.

10.2.3 WAF Exchange Web servers

Hinzufügen eines Web Servers über die entsprechende Konfiguration.

10.2.4 Firewall-Regel für WAF Autodiscover

Unter Regeln und Richtlinien → Firewall-Regeln → Firewall-Regel hinzufügen muss für jeden Pfad der Exchange Server und die Authentifizierung angepasst werden.

10.2.5 Firewall-Regel für WAF Exchange Webservices

Für jeden Pfad müssen der Exchange Server und die Authentifizierung angepasst werden.

Die Ausnahme für MAPI oder RPC muss entsprechend konfiguriert werden. Ob MAPI oder RPC verwendet wird, hängt von der Umgebung ab.

10.2.6 Webproxy-Beschränkung anpassen

Wurde eine WAF für Exchange oder andere Dienste erstellt, sollte die Größenbeschränkung angepasst werden. Bei einem lokalen Exchange ist dies zwingend notwendig. Ohne Anpassung können extern (OWA, Mobilgeräte) keine E-Mails größer 1 MB versendet werden.

10.2.7 Anpassung von 1MB auf 50MB:

. Per SSH an der Firewall anmelden

. Menüpunkt 5 "Device Management" wählen

. Punkt 3 "Advanced Shell" auswählen

. Befehl eingeben:

```
psql -U nobody -d corporate -c "select name,id,sec_request_body_no_files_limit from tblwaf
```

. ID der zu ändernden Profile notieren

. Upload-Limit festlegen (50MB = 52428800):

```
psql -U nobody -d corporate -c "update tblwafsecurityprofile set sec_request_body_no_files
```

. Einstellungen überprüfen

. reverseproxy.conf neu erstellen:

```
opcode waf_reconfig -t json -b '{"Entity": "waf_advanced_config", "Event": "UPDATE"}' -ds
```

Wichtiger Hinweis: Sobald die Policy über den Webadmin geändert wird, muss der Wert erneut gesetzt werden.

11 Wireless-Einstellungen

11.1 Gast-WLAN

Bei der Nutzung eines Gast-WLANs wird empfohlen, die Client Isolation zu aktivieren. Dies verhindert die Kommunikation zwischen Gästen im WLAN.

Ein Gästenetzwerk muss ein getrennter Netzbereich sein und einer eigenen Zone zugewiesen werden. Der Zugriff auf das Produktivnetz muss unterbunden werden.

11.2 Fast Transition

Bei der Nutzung mehrerer Access Points wird die Aktivierung von Fast Transition empfohlen. Dies ermöglicht einem Endgerät den Wechsel zu einem Access Point mit besserer Qualität, bevor die Verbindungsqualität schlechter wird.

12 E-Mail-Konfiguration

Die Firewall sollte grundsätzlich im MTA-Modus betrieben werden. Im Folgenden wird eine Best Practice-Konfiguration beschrieben.

12.1 MTA-Modus aktivieren

Unter E-Mail → Allgemeine Einstellungen kann der MTA-Modus aktiviert werden. Folgende Einstellungen müssen in den allgemeinen Einstellungen getroffen werden:

12.2 SMTP-Richtlinie erstellen

Unter E-Mail → Richtlinien & Ausnahmen:

Wenn als Maßnahme unter Spam "Quarantäne" ausgewählt ist, muss diese auch konfiguriert werden. Bei FullGuard Plus muss Sandstorm aktiviert werden.

12.3 SMTP Routing im MTA-Modus

Bei mehreren Internetleitungen oder externen IP-Adressen kann es notwendig sein, den ausgehenden Mailverkehr an eine Schnittstelle und externe IP zu binden. Je nach Bedarf muss eine NAT-Regel und eine SD-WAN-Policy erstellt werden.

12.4 Richtlinie für Microsoft 365

Bei Exchange-Hybrid muss eine zusätzliche Routing-Richtlinie erstellt werden, die die Microsoft 365- Domäne enthält und auf Exchange Online zeigt. Der Ziel-Host kann aus den MX-Einstellungen von Exchange Online entnommen werden.

13 E-Mail-Quarantäne

Für die Nutzung der Quarantäne ist es zwingend notwendig, die Benutzer aus dem Active Directory mit der XG zu synchronisieren. Die XG kann Quarantäne-E-Mails nur an bekannte Benutzer senden. Am einfachsten funktioniert dies mittels STAS Client, der auf allen Domain Controllern installiert werden muss.

Zusätzlich ist der Import von AD-Gruppen erforderlich. Für die Quarantäne sollte eine Gruppe existieren, in der sich alle Benutzer befinden (z.B. Domänenbenutzer).

13.1 Quarantäne aktivieren

Die Quarantäne muss entsprechend den Anforderungen aktiviert und konfiguriert werden.

Falls ein FQDN statt der IP der internen Schnittstelle genutzt werden soll, muss unter Verwaltung → Admin- und Benutzereinstellungen eine entsprechende Anpassung durchgeführt werden.

13.2 Quarantänebericht für AD-Gruppen erlauben

Nach Import der entsprechenden AD-Gruppe und STAS-Konfiguration muss in den Gruppen die Zustellung der Quarantäne-E-Mails eingestellt werden.

> **Wichtiger Hinweis:** Seit Firmware Version 17.5.0 funktionieren die Freigabe-Links in der Quarantäne-E-Mail nicht mehr. Eine Freigabe durch den Benutzer ist ausschließlich über das User Portal möglich.

14 E-Mail-Verschlüsselung

Sophos bietet die Möglichkeit, verschlüsselte PDF-Dateien zu versenden. Am einfachsten funktioniert dies mittels Outlook Add-in, das direkt bei Sophos heruntergeladen werden muss.

14.1 Erstellen einer SPX-Vorlage

Unter E-Mail → Verschlüsselung muss eine neue Vorlage erstellt werden.

14.2 Konfigurationsmöglichkeiten für das Passwort:

1. **Vom Absender festgelegt** - Der Absender fügt folgenden String in den Betreff ein: [secure:PW]
2. **Einmalkennwort für jede E-Mail generieren** - Der Absender bekommt das Passwort zugeschickt
3. **Generieren und für Empfänger gespeichert** - Der Absender bekommt das Passwort zugeschickt; wird je nach Konfiguration gespeichert
4. **Vom Empfänger festgelegt** - Diese Variante funktioniert seit Firmware Version 17.5.0 nicht mehr

Der Text unter "Anweisung für Empfänger" muss entsprechend angepasst werden.

14.3 Vorlage auswählen und Passwort-Speicherung festlegen

Die Standard-SPX-Vorlage muss ausgewählt werden. Zusätzlich kann festgelegt werden, wie lange das Passwort auf der Firewall gespeichert wird (nur bei "Generieren und für Empfänger gespeichert").

14.4 Verschlüsselte E-Mail mit Outlook versenden

Der Benutzer verwendet den Verschlüsseln-Button. Bei der Variante "Vom Absender festgelegt" muss folgender String in den Betreff eingefügt werden: [secure:Passwort] (wobei "Passwort" entsprechend ersetzt werden muss).

15 Relay-Einstellungen

Je nach Umgebung ist es notwendig, die Relay-Einstellungen zu ändern.

Unter E-Mail → Relay-Einstellungen kann beispielsweise der lokale Exchange hinterlegt und eine Authentifizierung eingerichtet werden.

16 Externer Mailempfang

16.1 Mailempfang von extern aktivieren

Damit E-Mails von extern per MX empfangen werden können, muss in der Verwaltung SMTP-Relay aktiviert werden.

17 Central Synchronisation

Die Central Synchronisation sollte wenn möglich aktiviert werden. Je nach Lizenzmodell muss die XG mit dem entsprechenden Sophos Central Account verbunden werden.

Die Einrichtung der Sophos Central Firewall-Verwaltung ist über einen OTP-Token möglich und stellt die empfohlene Best Practice dar.

17.1 Registrierung mit Sophos Central

Um den Mehrwert von Synchronized Security zu nutzen, Verwaltbarkeit über das Sophos Central Dashboard, Nutzung von Security Heartbeat, Application Control, Reporting und Sicherungen zu ermöglichen, ist die Anbindung an das Sophos Central Portal erforderlich.

18 VPN-Konfiguration

Wichtiger Hinweis: PPTP-VPN nicht mehr verwenden!

18.1 SSL-VPN einrichten (Client-Zugriff)

Wählen Sie VPN → VPN-Einstellungen anzeigen.

Hier können grundlegende Einstellungen wie DNS-Server, Domäne und Verschlüsselung angepasst werden.

Unter SSL-VPN (Fernzugriff) muss eine neue Richtlinie erstellt werden.

Im Bereich "Mitglieder der Richtlinie" werden alle Benutzergruppen oder Benutzer ausgewählt, die SSL- VPN-Zugriff erhalten sollen. Nur hier eingetragene Benutzer können sich die Konfiguration über das User Portal herunterladen.

Unter "Zugelassene Netzwerkressourcen" werden die Netzwerke eingetragen, auf die zugegriffen werden soll.

Abschließend muss eine passende Firewall-Regel erstellt werden. Jeder berechtigte Benutzer kann sich am User Portal anmelden und seine persönliche VPN-Konfiguration herunterladen.

18.2 Einrichtung Sophos Connect Client

Es wird empfohlen, zukünftig nur noch den Sophos Connect Client zu nutzen (SSL-Client wurde im Januar 2022 abgekündigt). Der Sophos Connect Client kann sowohl mit IPSec als auch per SSL-VPN eine Verbindung herstellen und per GPO verteilt werden.

Wichtige Hinweise:

- Es darf kein SSL-VPN Client auf dem Rechner installiert sein

- Für SSL-VPN muss die Konfiguration weiterhin über das User Portal heruntergeladen werden

18.3 Einrichtung auf der XG

Es gibt zwei Authentifizierungsmöglichkeiten: PSK oder Zertifikat. Für die Zertifikat-Authentifizierung muss zunächst ein Zertifikat unter "Zertifikate" → "Hinzufügen" erstellt werden.

Anschließend kann unter VPN → IPSec (Fernzugriff) die Einrichtung durchgeführt werden.

Nach Speicherung der Einstellungen können Client und Konfiguration direkt heruntergeladen werden.

18.4 Nachträgliche Anpassung der Konfigurationsdatei

Wurde bei der Einrichtung eine Schnittstelle mit vorgelagertem Router oder dynamischer IP ausgewählt, muss die heruntergeladene Konfigurationsdatei angepasst werden:

. Konfiguration mittels 7zip entpacken

. Nach dem Entpacken die *.scx-Datei mit Notepad++ öffnen

. Externen DNS-Namen oder IP eintragen

18.5 Installation und Verteilung der Konfiguration

. Sophos Connect installieren (bei automatischer Verteilung mit Schalter /qn)

. Konfigurationsdatei in den Pfad `C:\Program Files (x86)\Sophos\Connect\import` kopieren

Jeder berechtigte Benutzer kann sich mit seinen Zugangsdaten verbinden.

18.6 Import einer SSL-VPN Konfiguration in Sophos Connect

. Am User Portal anmelden und Konfiguration für andere Betriebssysteme herunterladen

. Sophos Connect Client starten und Konfiguration über den Import-Button importieren

19 Ransomware-Prävention

20

Bei der Konfiguration müssen die Präventionshinweise für Sophos-Produkte beachtet werden.

20.1 Empfohlene Einstellungen:

- **ATP:** Protect → Erweiterte Threat → Erweiterte Bedrohungsschutz: ON
- **Scan Engine:** Protect → Web → Allgemeine Einstellungen → Scan Engine-Auswahl → Dual Engine
- **HTTPS-Entschlüsselung:** In jeder relevanten Richtlinienregel → Web Malware und Content Scanning → Entschlüsseln & Scan HTTPS: ON

20.2 Webrichtlinie mit blockierten Kategorien:

-
  - Anonymisierer
  - Befehl & Kontrolle
  - Phishing & Betrug
  - Spam-URLs
- **IPS:** Protect → Intrusion Prevention → IPS-Richtlinien → Malware-Kommunikation

21 Zwei-Faktor-Authentifizierung

21.1 OTP-Dienste aktivieren

OTP-Dienste können unter Authentication → One-time password → Settings aktiviert werden.

21.2 Benutzer anlegen

Ein neuer Benutzer wird unter Authentication → Users → Add angelegt.

21.3 OTP-Token einrichten

Nach dem Anlegen des Benutzers im Admin-Portal kann sich dieser im User Portal anmelden. Nach erfolgreicher Anmeldung wird der OTP-Token zur Authentifikation angezeigt.

Der OTP-Token wird mittels Sophos Authenticator gescannt und eingerichtet. Der Sophos Authenticator beginnt mit der Erzeugung von OTP-Codes.

21.4 Anmeldung mit OTP

Nach dem Hinzufügen des QR-Codes zum Sophos Authenticator auf "Proceed to login" klicken. Bei der Anmeldung im User Portal das Kennwort in folgendem Format eingeben:

> **Format:** Passwort + 6-stelliger Code aus dem Sophos Authenticator
> **Beispiel:** <Benutzerkennwort><Erzeugter_Code>

> **Wichtiger Hinweis:** Die Uhrzeit des mobilen Endgeräts muss mit der aktuellen Zeit übereinstimmen, da der Token sonst falsch generiert wird.

22 Nützliche Links

Ressource	URL	Beschreibung
Sophos Release Notes	https://docs.sophos.com/releasenotes/	Aktuelle Versionshinweise und bekannte Probleme
Sophos Support Portal	https://support.sophos.com	Technischer Support und Knowledge Base
Sophos Community	https://community.sophos.com	Community-Forum für Erfahrungsaustausch
Sophos Documentation	https://docs.sophos.com	Offizielle Produktdokumentation

Hinweis: Diese Anleitung basiert auf Sophos XG Firewall Version 18.x und kann bei neueren Versionen Abweichungen aufweisen. Prüfen Sie vor der Implementierung die aktuellen Sophos Release Notes auf bekannte Probleme und Änderungen.

Sicherheitshinweis: Alle Konfigurationsschritte sollten zunächst in einer Testumgebung durchgeführt und validiert werden, bevor sie in der Produktionsumgebung implementiert werden.