

ITdesign ProtectIT Paket

Version 1.0



TAKE **IT** EASY

Konzeption und Inhalt: ITdesign

Nutzung durch Dritte nur mit schriftlicher Genehmigung von ITdesign

INHALTSVERZEICHNIS

1	ITDESIGN PROTECTIT	3
1.1	BETRIEBSSYSTEME / APPLIKATIONEN.....	3
1.2	SUBSCRIPTION SERVICES	3
1.3	FEATURES.....	3
2	MODULE.....	5
2.1	TMG – FIREWALL.....	5
2.2	TMG – WEBSECURITY GATEWAY (FORWARD PROXY)	5
2.3	TMG – WEBPUBLISHING GATEWAY (REVERSE PROXY).....	5
2.4	TMG – MAILSECURITY GATEWAY	6
2.5	TMG – ADD-ONS.....	6
3	NUTZEN FÜR DEN KUNDEN.....	7
4	ABGRENZUNG UND VORGABEN	8
4.1	ABGRENZUNG	8
4.2	VORGABEN.....	8
4.2.1	<i>Infrastruktur</i>	8
4.2.2	<i>Hardware</i>	9
4.2.3	<i>Lizenzen</i>	10
5	PROJEKTABLAUF.....	11
6	PREISGESTALTUNG.....	12

1 ITdesign ProtectIT

ITdesign hat ein Paket geschaffen, mit dem zu einem Fixpreis mittels Microsoft Threat Management Gateway (TMG), dem Nachfolger des MS ISA Servers, der Netzwerkzugang in das Unternehmen und aus dem Unternehmen geregelt wird.

Inhaltlich werden alle Möglichkeiten der Lösung dargestellt und im Zuge der Implementierung umgesetzt. Die Auswahl der Funktionen, die tatsächlich beim Kunden aktiviert werden, erfolgt nach der weiter unten im Text dargestellten Liste.

Ziel ist es, nach Installation der Lösung einen sicheren Zugriff für Mobile Worker auf Unternehmensressourcen zu gewährleisten und das Unternehmen hinsichtlich Virenschutz und https Traffic bestmöglich abzusichern. Weiters sind dadurch die internen Mitarbeiter vor den im Internet lauernden Gefahren geschützt.

1.1 Betriebssysteme / Applikationen

Die Lösung wird auf Basis **MS Windows 2008** und **MS Forefront TMG (Threat Management Gateway)** installiert. Entsprechend der Modulauswahl (nur Firewall-Komponente, nur Proxy-Komponente, etc.) kann die Installation entweder auf einem physischen Server oder in einer virtuellen Umgebung erfolgen.

1.2 Subscription Services

Je nach gewünschten Funktionen werden entsprechende Update Services konfiguriert, die die aktuellen Signaturen automatisch aus dem Internet beziehen.

1.3 Features

Features - externe User	
	Microsoft Exchange Zugang für WEB Access Microsoft Exchange Zugang für Outlook Microsoft Exchange Zugang für Mobile Devices Web Server Publishing Sharepoint Publishing Client-VPN über SSL (SSTP)
Features - interne User	
	Caching Proxy Server Virenschanning / Download Security AntiPhising / Malware Schutz HTTPS Content Inspection Firewall Client für erweiterte Funktionen
Features - Admins	
	Intelligent Application Layer Gateway Firewall Network Inspection System SMTP / eMail Publishing mit Virenschanning und AntiSpam

	Funktionalität
Features - Optional	
	RSA Integration Integriertes Loadbalancing für Publishing von internen WEB Servern Loadbalancing Cluster Möglichkeit mit Management Server

2 Module

Sämtliche Module werden voneinander losgelöst betrachtet und können auch dementsprechend implementiert werden.

2.1 TMG – Firewall

- Planung (Erfassung der bestehenden Netzwerktopologie, Definition der IP-Adressen, Exportieren der Regeln, etc.)
- Installation & Konfiguration von MS Forefront TMG
- Übernahme bzw. Implementierung von max. 20 Firewall-Regeln
- Übernahme bzw. Implementierung von max. 2 Site-To-Site VPN Verbindungen
- Implementierung eines SSL-VPN Zugangs (via Secure Sockets Tunneling Protocol) und Einrichtung des VPN-Clients auf max. 2 Clients (Windows XP SP3, Windows Vista, Windows 7)
- Inbetriebnahme & Testbetrieb der Konfiguration
- Dokumentation

2.2 TMG – WebSecurity Gateway (Forward Proxy)

- Planung (Definition der unterschiedlichen Security Gruppen, Definition der URL-Kategorien, etc.)
- Installation & Konfiguration von MS Forefront TMG
- Übernahme bzw. Implementierung von max. 5 benutzergruppenbezogenen WebSecurity-Regeln inklusive URL-Filtering und Malware- bzw. HTTPS-Inspection
- Inbetriebnahme & Testbetrieb der Konfiguration
- Dokumentation

2.3 TMG – WebPublishing Gateway (Reverse Proxy)

- Planung (Konfiguration Exchange überprüfen, etc.)
- Installation & Konfiguration von MS Forefront TMG
- Konfiguration der Regel für Outlook Web Access (OWA)
- Konfiguration der Regel für Outlook AnyWhere inkl. Konfiguration von max. 2 Clients für Verbindungstests
- Konfiguration der Regel für Exchange ActiveSync inkl. Konfiguration von max. 2 Mobile Devices für Verbindungstests (Mobile Devices müssen für die jeweilige Konfiguration-Option unterstützt sein)
- Implementierung von max. 2 Regeln für das Veröffentlichen eines Web-Servers
- Implementierung von max. 2 Regeln für das Veröffentlichen eines Sharepoint-Servers
- Inbetriebnahme & Testbetrieb der Konfiguration
- Dokumentation

2.4 TMG – MailSecurity Gateway

- Planung
- Installation & Konfiguration von MS Forefront TMG
- Konfiguration der Regel für SMTP-Relay inkl. AntiSpam und Malware-Inspection
- Inbetriebnahme & Testbetrieb der Konfiguration
- Dokumentation

2.5 TMG – Add-ons

- Installation des TMG Firewall Clients auf max. 2 Clients und Konfiguration einer entsprechenden Regel
- Forefront TMG Enterprise Edition inkl. Management Server und integriertem Network Load Balancing
 - Installation & Konfiguration eines dedizierten Configuration Storage Server (Management Server zur Verwaltung des Rule-Set)
 - Installation & Konfiguration von ADAM (Active Directory Application Mode) und eines SQL-Servers (MS SQL Server 2008 Express oder MS SQL Server 2008) für die Logging-Funktionalität
 - Konfiguration der beiden Nodes in einem Network Load Balancing Cluster Verbund (Integrated Mode)
- Integration der RSA SecurID Token Authentifizierung

3 Nutzen für den Kunden

Durch die Realisierung dieser Lösung von ITdesign ergibt sich folgender Nutzen:

- Ablöse von vielen Zusatzprodukten – Verringerung der Kosten und des administrativen Aufwands
- Homogenisierung und Vereinfachung der Infrastruktur
- Prüfung des Internet Datenstroms (Url checken und https Traffic)
- Verhindern, dass Trojaner etc. über Internet ins Unternehmen gelangen
- Virenschutz selbst bei https Traffic, wie man es vom Mail gewohnt ist
- Lastverteilung von WEB Services – Performancegewinn
- Erhöhung der Verfügbarkeit für alle auf TMG zusammengefasste Schutzprogramme
- Schutz der Server, selbst wenn ein Security Hotfix noch nicht flächendeckend ausgerollt ist
- VPN über HTTPS und damit wiederum Reduzierung der Zusatzprodukte

4 Abgrenzung und Vorgaben

Im folgenden Abschnitt wird eine exakte Abgrenzung der Inhalte, die in der Pauschale enthalten sind, beschrieben. Des Weiteren werden die benötigten Anforderungen bzw. Vorgaben für die Kundenumgebung definiert.

4.1 Abgrenzung

- Die Implementierung findet nur für einen Standort statt
- Die Lösung wird ausschließlich in englischer Sprache installiert
- Im Zuge der Implementierung werden max. 2 VPN-Clients und max. 2 Mobile Devices getestet

4.2 Vorgaben

Die folgenden Voraussetzungen müssen in der Kunden Umgebung gegeben sein, um ProtectIT einzuführen. Sind diese nicht vorhanden, muss der Kunde die entsprechenden Voraussetzungen schaffen bzw. ITdesign damit extra beauftragen.

4.2.1 Infrastruktur

ITdesign geht bei der Implementierung immer von einer voll funktionsfähigen Basis Infrastruktur aus. Die Dienste DNS, DHCP, Directory Services (Active Directory) und entweder eine interne Certification Authority (CA) oder die Möglichkeit zur Ausstellung von offiziellen Zertifikaten müssen zur Verfügung stehen. Netzwerk, Exchange und alle weiteren beteiligten Dienste laufen fehlerfrei und sind entsprechend konfiguriert.

Modul	Voraussetzungen
TMG - Firewall	Physischer Windows Server 2008 (x64) oder Windows Server 2008 R2 (x64) Standard oder Enterprise Edition Mindestens 2 Netzwerk Anschlüsse Zur Verfügung stehende IP-Adressen Netzwerk / Switch Konfiguration Entsprechende Clients für die Einrichtung von SSL-VPN (Windows XP SP3, Windows Vista oder Windows 7)
TMG – WebSecurity Gateway (Forward Proxy)	Physischer oder virtueller Windows Server 2008 (x64) oder Windows Server 2008 R2 (x64) Standard oder Enterprise Edition Mindestens 1 Netzwerk Anschluss Zur Verfügung stehende IP-Adresse(n) Netzwerk / Switch Konfiguration Für die HTTPS-Inspection wird eine interne Certification Authority (CA) zur Ausstellung von Zertifikaten benötigt
TMG – WebPublishing	Physischer oder virtueller Windows Server 2008 (x64)

Gateway (Reverse Proxy)	<p>oder Windows Server 2008 R2 (x64) Standard oder Enterprise Edition</p> <p>Mindestens 1 Netzwerk Anschluss</p> <p>Zur Verfügung stehende offizielle IP-Adresse(n)</p> <p>Exchange 2003/SP2 oder Exchange 2007/SP1 - Umgebung entsprechend vorkonfiguriert (FrontEnd Server oder Client Access Server vorhanden)</p> <p>Für die SSL-Verbindung sind entweder offizielle Zertifikate vorhanden oder es ist eine interne Certification Authority (CA) vorhanden</p> <p>Für die Veröffentlichung von WebServern müssen entweder der MS Internet Information Server oder ein Apache Web Server zum Einsatz kommen</p> <p>Für die Veröffentlichung von Sharepoint muss ein entsprechender Sharepoint Server verfügbar sein</p> <p>Für die Tests von Outlook Anywhere müssen 2 Windows Clients inklusive Outlook zur Verfügung gestellt werden</p> <p>Für die Tests von Exchange ActiveSync werden 2 unterstützte ActiveSync Mobile Devices benötigt</p>
TMG – MailSecurity Gateway	<p>Physischer oder virtueller Windows Server 2008 (x64) oder Windows Server 2008 R2 (x64) Standard oder Enterprise Edition</p> <p>Mindestens 1 Netzwerk Anschluss</p> <p>Zur Verfügung stehende IP-Adresse(n)</p> <p>Netzwerk / Switch Konfiguration</p> <p>Es kann jegliche Art von SMTP Server veröffentlicht werden</p>

4.2.2 Hardware

Alle Module außer „TMG – Firewall“ können sowohl auf einem virtuellen als auch auf einem physischen Server realisiert werden. Außer sicherheitstechnischen Überlegungen sollte das Modul „TMG – Firewall“ unbedingt auf einem physischen Server umgesetzt werden.

Es müssen, je nachdem welche Module implementiert werden, bis zu 3 Netzwerkkarten, die in die entsprechenden Netze gepatcht sind, zur Verfügung stehen (internes Netzwerk, DMZ, externes Netzwerk).

Alle Module haben folgende hardwarespezifischen Mindestanforderungen:

- Processor: Pentium* IV 2.8 GHz x64
- 4 GB RAM
- 30GB SystemDisk

4.2.3 Lizenzen

Die notwendigen Lizenzen (Windows Server 2008 und Forefront TMG) werden vom Kunden bereitgestellt. Für die Subscriptions für Antivirus, Malware und AntiSpam sind entsprechende Verträge abzuschließen.

(→ Sollte der Kunde in diesem Punkt Beratung benötigen, ist ITdesign hier bei der Auswahl gerne behilflich)

Forefront TMG wird entweder auf physischer Hardware oder in einer von Microsoft unterstützten virtuellen Umgebung nach den mit dem Kunden vereinbarten Vorgaben installiert (Empfehlung für virtuelle Umgebungen: Microsoft Hyper-V oder VMware ESX Server).

Als Betriebssystem kommt Windows 2008 in der 64Bit Version zum Einsatz. Dieses ist vom Kunden entsprechend zu lizenzieren. Ist vom Kunden Microsoft Exchange WEB Publishing gewünscht, wird der Exchange 2003 Frontend Server bzw. der Exchange 2007 Client Access Server entsprechend konfiguriert.

5 Projektablauf

Das ProtectIT Implementierungsprojekt wird in folgende Teile gegliedert:

- **ProtectIT Fragenkatalog**
ITdesign übergibt nach der Beauftragung einen Fragenkatalog, welcher die wichtigsten Punkte des ProtectIT Projektes behandelt. Der Fragenkatalog wird von Kunden ausgefüllt zurück an ITdesign gesendet. Aufgrund des Fragenkatalogs wird von ITdesign das Kickoff Meeting vorbereitet.
- **ProtectIT Kickoff Meeting**
Im Kickoff Meeting wird der vom Kunden ausgefüllte Fragenkatalog besprochen; etwaige Unklarheiten werden beseitigt. Anschließend wird der Zeitplan ausgearbeitet und fixiert. Die Ergebnisse des Kickoff Meetings werden in einem Protokoll festgehalten.
- **Kundenvorbereitungen**
Nach dem Kickoff Meeting hat der Kunde Zeit, die entsprechenden Vorbereitungen in der Infrastruktur durchzuführen. Die notwendigen Schritte werden im Zuge des Kickoff Meetings besprochen und festgelegt.
- **Umsetzung ProtectIT**
Nach Abschluss der notwendigen Vorarbeiten des Kunden beginnt ITdesign mit der ProtectIT Umsetzung lt. Angebot bzw. Kickoff Meeting.
- **Übergabe, Dokumentation & Testphase**
Sobald die Arbeiten von ITdesign abgeschlossen sind, wird die erstellte ProtectIT Implementierung anhand der erstellten Dokumentation an den Kunden übergeben. Im Anschluss an die Übergabe hat der Kunde entsprechend Zeit, die Implementierung zu testen und etwaige Probleme an ITdesign zu melden.
- **Korrekturarbeiten**
Nach der Testphase werden von ITdesign die gewünschten Änderungen eingearbeitet. Die durchgeführten Arbeiten werden in der vorhandenen Dokumentation festgehalten und dem Kunden demonstriert.
- **Abnahme**
Im Anschluss an die Korrekturarbeiten wird das Projekt vom Kunden abgenommen und von ITdesign verrechnet.

6 Preisgestaltung

Modul	Preis
TMG - Firewall	5.280,-
TMG – WebSecurity Gateway (Forward Proxy)	2.640,-
TMG – WebPublishing Gateway (Reverse Proxy)	3.300,-
TMG – MailSecurity Gateway	2.970,-
TMG – Add-ons - Forefront TMG Enterprise Edition inkl. Management Server und integriertem Network Load Balancing	1.320,-

Beim Kauf von mehreren Modulen werden ab dem zweiten Modul jeweils 500,- EURO abgezogen (betrifft pro Modul die Installation & Konfiguration sowie die Inbetriebnahme & Testbetrieb).