Systemkonfiguration (config)

Das Konfigurationsmenü ist das Herzstück der mp-Firewall. Hier werden sämtliche Einstellungen vorgenommen, die die Funktionsfähigkeit sicherstellen. Die Firewall ist ein sehr robustes "Arbeitstier", welches nach der einmaligen Einrichtung wenig Wartungsaufwand benötigt. Sollten dennoch einmal neue Netzwerk-Einstellungen vorgenommen werden müssen oder wird eine Konfiguration geändert, so bedarf dies nur in den wenigsten Fällen eines Neustarts des Systems. Speziell zur Vermeidung von Ausfallzeiten wurde dazu ein doppeltes Anwendungsverfahren entwickelt.

Voll Anwenden vs. Sanft Anwenden
Während das volle Anwenden eine neue Konfiguration sofort in das System übernimmt und sämtliche Dienste neu startet (dabei werden auch bestehende Verbindungen abgebrochen), so werden über das sanfte Anwenden nur die Konfigurationsdateien neu geschrieben und diejenigen Dienste neu gestartet, deren Neustart keine laufenden Benutzerverbindungen abbricht. Beim nächsten vollen Anwenden oder nach dem Neustart sind dann ebenfalls alle Einstellungen voll wirksam. In den meisten Fällen reicht das sanfte Anwenden.

Systemeinstellungen

Um die Systemeinstellungen zu ändern bitte als *config* anmelden. Unter *Einstellungen* > *Systemeinstellungen* werden die grundsätzlichen Angaben zum Hostnamen, Domains etc. eingetragen. Diese müssen bei der Einrichtung der mp-Firewall einmalig eingerichtet werden. Es gibt in dem Menü folgende Einstellungsmöglichkeiten:

Menüpunkt	**Beschreibung**
Hostname	Name der Firewall für das Netzwerk. Mit diesem Namen ist es möglich die Firewall direkt mit dem Namen anzusprechen und nicht nur per IP-Adresse.
Domain	Name der Domain, die für das Netzwerk gilt. Die Domain beschreibt einen zusammenhängenden Teilbereich des hierarchischen DNS Namensraumes. Eine Domain umfasst ausgehend vom dem Domainnamen immer die gesamte untergeordnete Baumstruktur.
Mail-Domain	Name der Mail-Domäne für den integrierten Mailserver auf der Firewall. Falls es mehrere Mail-Domänen gibt, können diese durch ein Leerzeichen getrennt eingeben werden. Die erste Domäne wird automatisch zur Standard-Domäne.
HELO-Name	SMTP-HELO-Name dieses Servers für den Mailversand.
Maximale Mailgröße	Hier können Sie die maximal erlaubte Mail-Größe eintragen. Der Wert kann zwischen 0 und 20480000 liegen, was einer maximalen Mailgröße von 20 MB entspricht. Achtung: Wenn Sie die Spam-Verwaltung mit Maia Mailguard verwenden, müssen Sie die maximale Größe als Administrator dort ebenfalls einstellen!
Mailversand von außen	Ist dieser Schalter aktiviert, können nach einer SMTP-Authentisierung mit Benutzername und Passwort eines gültigen Accounts auf der Firewall auch über die externe Netzwerkschnittstelle E-Mails über den Mailserver der Firewall versendet werden.
Lokaler Namens-Trenner	Trennzeichen zwischen lokalem Namen und Erweiterung.
Aktion bei Strg-Alt-Entf	Aktion, die beim Drücken der Tastenkombination Strg-Alt-Entf ausgelöst wird.

Menüpunkt	Beschreibung
Statusreport-Empfänger	E-Mail Adresse an den der verschlüsselte Statusreport täglich versandt wird.
Statusreport-Absender	Absender-Adresse der täglich an den Support gesendeten verschlüsselten Statusreport E-Mail. Die Angabe kann notwendig sein, wenn Mailserver die Gültigkeit der Absende-Adresse prüfen.
Updatereport-Empfänger	E-Mail-Adresse für den Empfang der wöchentlichen Mail mit einer Übersicht von verfügbaren Updates für die Firewall. Mehrere Empfänger sind durch Leerzeichen zu trennen.
Stick-Sync zulassen	Zur Synchronisation mit einem zweiten System "Warm-Stand-By“ muss diese Option aktiviert sein.
Syslog-Lebensdauer	Anzahl der Tage, die Mail- und Systemlogs aufbewahrt werden. Die Rotation der Logs erfolgt immer täglich.
Doppelanmeldung nötig	Auswahl ob alle Einstellungen von Administratoren revisionssicher protokolliert werden sollen. Details dazu finden Sie im nachfolgenden Abschnitt.

Revisionssicheres Arbeiten
Sensitive Eingriffe, wie die Fernwartung oder die Fehlerbehebung in produktiven Systemen sollten einer revisionssicheren Protokollierung unterliegen. Dies bedeutet insbesondere, dass nachträgliche Änderungen oder das Löschen von Protokolldateien nicht unkontrolliert möglich sein dürfen. Die TightGate-Firewall unterstützt die Revisionsssicherheit durch das Konzept der Doppelanmeldung. Unter der Doppelanmeldung wird verstanden, dass ein Systembenutzer, der administrativ tätig wird, sich zusätzlich noch als "normaler" Benutzer autorisieren muss. Damit ist gewährleistet, dass nachvollzogen werden kann, welcher Benutzer gerade in seiner Funktion als Systemadministrator tätig geworden ist. Ist die Doppelanmeldung aktiviert wirkt sie auf folgende Benutzerrollen: *security*, *root*, *config*, *maint*, *backuser*, *update* und *revision*.

ACHTUNG: Wenn Sie alle Einstellungen vorgenommen haben verlassen die das Menü. Speichern Sie nun alle Änderungen über den Menüpunkt *Speichern* ab und wenden Sie diese mit dem Menüpunkt *Sanft Anwenden* an. Erst nach dem Anwenden werden die neuen Einstellungen wirksam.

Internes Netzwerk

Um das interne Netzwerk zu konfigurieren, melden Sie sich bitte als Benutzer *config* an und wählen Sie aus dem Menü den Menüpunkt *Einstellungen > Internes Netzwerk* aus. Es gibt folgende Einstellungsmöglichkeiten:

Menüpunkt	Beschreibung
Interfaces	Anzeige aller im System verfügbaren Netzwerk-Interfaces.
Netzwerk-Treiber (intern)	Auswahl des Netzwerkkarten-Treibers für das erste interne Netzwerkinterface.
MAC-Adresse (intern)	Auswahl der zugehörigen MAC-Adresse für das Netzwerkinterface.
MTU des Anschlusses (intern)	Die Maximum Transmission Unit (MTU) beschreibt die maximale Paketgröße, die über ein Netzwerk übertragen werden kann, ohne dass das Datenpaket fragmentiert werden muss. Die MTU wird in Bytes angegeben. Wenn Sie nicht genau wissen, welcher Wert einzutragen ist, lassen Sie dieses Feld leer.

Menüpunkt	Beschreibung
IP-Adresse (intern)	Die IP-Adresse der mp-Firewall für das interne Netz. Über diese IP-Adresse kommuniziert das interne Netz mit der Firewall.
IP-Netzwerk-Valid-Bits (intern)	Anzahl der gültigen IP-Netzwerk-Bits des internen Netzes.
IP-Netzwerk-Maske (intern)	Einstellung der Netzwerk-Maske entsprechend dem IP-Adressbereich.
IP-Netzwerk (intern)	IP-Netzwerk dieses Servers.
IP-Broadcast (intern)	Broadcast-Adresse für das IP-Netzwerk dieser Firewall.
IP-Netzwerk rückwärts (intern)	IP-Netzwerk der Firewall rückwärts ohne die Hosts.
IP-Adresse Hostanteil (intern)	Hostanteil der IP-Adresse des Servers.
Weitere IP-Netze (intern)	Hier können weitere Klienten-Netze, die im internen Netz über Router angeschlossen sind, konfiguriert werden.
——–	
DHCP minimum IP	Erste IP-Adresse für die Vergabe per DHCP. Wird die Einstellung für "DHCP minimum" und "DHCP maximum" leer gelassen so erfolgt keine DHCP-Adressvergabe durch die Firewall.
DHCP maximum IP	Letzte IP-Adresse für die Vergabe per DHCP. Wird die Einstellung für "DHCP minimum" und "DHCP maximum" leer gelassen so erfolgt keine DHCP-Adressvergabe durch die Firewall.
DHCP feste Adressen	Zuordnung von MAC-Adressen einzelner Netzwerkgeräte zu festen IP-Adressen. Die zugeordnete IP-Adresse darf nicht innerhalb des von der Firewall per DHCP vergebenen IP-Adressbereichs liegen.
DHCP-Adressen in DNS eintragen	Auswahl, ob alle Rechner mit dynamischen IP-Adressen über DHCP auch mit DNS-Standard-Namen erreichbar sein sollen. Dieses wird manchmal für Dienste anderer Server benötigt.

ACHTUNG: Wenn Sie alle Einstellungen vorgenommen haben verlassen die das Menü. Speichern Sie nun alle Änderungen über den Menüpunkt *Speichern* ab und wenden Sie diese mit dem Menüpunkt *Voll Anwenden* an. Erst nach dem Anwenden werden die neuen Einstellungen wirksam.

Externes Netzwerk

Das externe Netzwerk ist der Zugang zum Internet. Hier werden alle Einstellungen vorgenommen, die für die Welt außerhalb Ihres Unternehmens relevant sind.

Um das externe Netzwerk zu konfigurieren, melden Sie sich bitte als Benutzer *config* an und wählen Sie aus dem Menü den Menüpunkt *Einstellungen > Externes Netzwerk* aus. Sie haben folgende Einstellungsmöglichkeiten:

Menüpunkt	Beschreibung
Interfaces	Anzeige aller im System verfügbaren Netzwerkinterfaces.
—	
Von aussen offene TCP-Ports	Auswahl diejenigen TCP-Port, die für alle Verbindungen aus dem Internet geöffnet sein sollen.
Von aussen offene UDP-Ports	Auswahl diejenigen UDP-Port, die für alle Verbindungen aus dem Internet geöffnet sein sollen.

Menüpunkt	Beschreibung
IP-Adressen der Fernwartung	Bitte hier die IP-Adressen derjenigen Rechner eintragen, die für eine Fernwartung per SSH zugelassen werden sollen. Die IP-Adresse(n) sind in der Form a.b.c.d/n anzugeben. Mehrere IP-Adressen sind mit Leerzeichen voneinander zu trennen. Ist keine Fernwartung vorgesehen, so bleibt dieses Feld leer. Hinweis: Sind hier IP-Adressen eingetragen, so ist für diese der SSH-Port von außen schon freigegeben. Es ist NICHT! notwendig den SSH-Port von außen allgemein zu öffnen.
—	
Netzwerk-Treiber (extern)	Auswahl des Netzwerkkarten-Treibers für das externe Netzwerkinterface.
MAC-Adresse (extern)	Auswahl der zugehörigen MAC-Adresse für das Netzwerkinterface.
Art des Anschlusses (extern)	Sie können auswählen, ob Sie einen direkten Netzwerkzugang haben oder ob Sie über einen DSL-Anschluss mit PPPoE mit dem Internet verbunden sind. Bei der Auswahl von DSL erscheinen im unteren Abschnitt noch Menüpunkte zur Einstellung der Zugangsdaten für das DSL.
Upload-Rate des Anschlusses (extern)	Sie können hier die Upload-Rate für den Internetzugang beschränken. Dieses ist besonders bei einigen DSL-Modems sinnvoll, deren Sendepuffer ausgehende Pakete ungünstig verteilt. Standardwert ist 0 für keine Begrenzung.
MTU des Anschlusses (extern)	Die Maximum Transmission Unit (MTU) beschreibt die maximale Paketgröße, die über ein Netzwerk übertragen werden kann, ohne dass das Datenpaket fragmentiert werden muss. Die MTU wird in Bytes angegeben. Für den Standardwert das Feld bitte leer lassen.
MSS an MTU binden (extern)	Auswahl, ob die MSS (Maximum Segment Size) an die maximale Paketgröße gebunden werden soll. Die MSS definiert die maximale Anzahl von Bytes, die als Nutzdaten in einem TCP-Segment versendet werden können. Standardauswahl ist Nein.
IP-Adresse (extern)	Die IP-Adresse der mp-Firewall für das externe Netz. Über diese IP-Adresse ist die Firewall aus dem Internet zu erreichen. Wenn Sie diesen Eintrag leer lassen, versucht das System eine Adresse über DHCP zu bekommen.
IP-Netzwerk-Valid-Bits (extern)	Anzahl der gültigen IP-Netzwerk-Bits des externen Netzes.
IP-Netzwerk-Maske (extern)	Entsprechend dem IP-Adressbereich die IP-Netzwerkmaske für das externe Netz.
IP-Netzwerk (extern)	IP-Adressbereich für das externe Netzwerk.
IP-Broadcast (extern)	Externe Broadcast-Adresse für das IP-Netzwerk dieser Firewall.
IP-Gateway (extern)	Sollte zwischen dieser Firewall und dem Internet noch ein weiteres Gateway stehen, so ist hier die IP-Adresse des zwischengeschalteten Gateways einzutragen.
DSL-Benutzer (extern)	Benutzername für den DSL-Zugang. (Wenn Sie die DSL-Kennung ändern wollen beachten Sie bitte den FAQ-Eintrag zu DSL)
DSL-Passwort (extern)	DSL-Benutzerpasswort für den DSL-Zugang.
DSL-Verbindungs-Timeout (extern)	Angabe nach wie vielen Sekunden die DSL-Verbindung von der Firewall getrennt werden soll, wenn keine Aktivität mehr festgestellt wird. Soll die DSL-Verbindung nicht getrennt werden, so bleibt diese Feld leer.

Menüpunkt	Beschreibung
DSL-Zwangstrennungszeiten (extern)	Angabe der vollen Uhrzeit-Stunde, zu denen die DSL-Verbindung regelmäßig von der Firewall getrennt werden soll. Soll keine Zwangstrennung vorgenommen werden bittet dieses Feld leer lassen.
DynDNS-Name (extern)	Angabe des DynDNS-Namenseintrags. Wird kein DynDNS verwendet, so bleibt dieses Feld leer.
DynDNS-Server (extern)	Angabe des DynDNS Nameservers. Der Standard-Eintrag members.dyndns.org bezeichnet den Standardserver für DynDNS.com, dieser wird bei einem anderen Dienst abweichen.
DynDNS-Login (extern)	Wird ein DynDNS verwendet, so ist hier der Login-Name einzutragen.
DynDNS-Passwort (extern)	Wird ein DynDNS verwendet, so ist hier das Passwort einzutragen.

ACHTUNG: Wenn Sie alle Einstellungen vorgenommen haben verlassen die das Menü. Speichern Sie nun alle Änderungen über den Menüpunkt *Speichern* ab und wenden Sie diese mit dem Menüpunkt *Voll Anwenden* an. Erst nach dem Anwenden werden die neuen Einstellungen wirksam.

Port-Durchleitung vom internen Netz ins Internet

Die Einstellungen der Durchleitung von Verbindungen aus dem internen Netzwerk regelt den direkten Zugriff aller Arbeitsplatz-Rechner in das Internet. Beachten Sie, dass über alle durchgeleiteten Ports die Arbeitsplätze direkt mit dem Internet kommunizieren können. So können Proxies ggf. wirkungslos werden. Sollen die Durchleitungen nur für einzelne Rechner freigegeben werden, so kann dies über den Menüpunkt Eigene Firewall-Regeln eingerichtet werden.
Zur Einstellung von Port-Durchleitungen wählen Sie bitte als *config* den Menüpunkt *Einstellungen* > *Durchleitungen* aus.

Folgende Einstellungsmöglichkeiten sind für die globalen Netzwerk-Durchleitungen des internen Netzwerkes in das Internet möglich:

Menüpunkt	Beschreibung
Maskierte TCP-Ports	TCP-Ports (Ziel-Ports) im Internet, die für das gesamte interne Netzwerk durchzuleiten sind.
Ping ICMP durchleiten	Erlaubnis von ICMP-Anfragen (Ping) aus dem internen Netzwerk in das Internet.
FTP-Klienten	Rechnern aus dem internen Netz mit freiem FTP-Zugriff ins Internet ohne Proxy.
FTP-Server	Einschränkung der erreichbaren FTP-Server für die eingetragenen FTP-Klienten. Wird kein Server oder Netzwerk eingetragen, werden alle Adressen freigeschaltet.
HBCI-Klienten	HBCI-Klienten, die direkt mit den unter HBCI-Servern eingetragenen HBCI-Servern über den HBCI-Port 3000 kommunizieren dürfen.
HBCI-Server	Liste von HBCI-Banking-Servern.
Elster-Klienten	Elster-Klienten, die direkt mit den unter Elster-Servern eingetragenen Servern über den Elster-Port 8000 kommunizieren dürfen.
Elster-Server	Liste von Elster-Servern zur elektronischen Kommunikation mit dem Finanzamt.

Bei den Punkten für FTP-, HBCI- und Elster-Klienten können mehrere IP-Adressen eingetragen werden. Diese sind dann jeweils durch ein Leerzeichen voneinander zu trennen.

ACHTUNG: Wenn Sie alle Einstellungen vorgenommen haben verlassen die das Menü. Speichern Sie nun alle Änderungen über den Menüpunkt *Speichern* ab und wenden Sie diese mit dem Menüpunkt *Sanft Anwenden* an. Erst nach dem Anwenden werden die neuen Einstellungen wirksam.

Uplink Server

Uplink Server sind Server, die von der mp-Firewall als zusätzliche "Quellen" herangezogen werden. Seien es nun Dienste wie Nameserver, Timeserver, ein übergeordneter Proxy oder auch Mail Relay Dienste. Hier können Sie die übergeordneten Informationsquellen der TightGate-Firewall festlegen.

Um die Einstellungen der Uplink-Server vorzunehmen, melden Sie sich bitte als Benutzer *config* an und wählen dann aus dem Menü *Einstellungen* > *Uplink Server* aus. Sie haben folgende Einstellungsmöglichkeiten:

Menüpunkt	**Beschreibung**
Nameserver 1	IP-Adresse des ersten Nameservers.
Nameserver 2	IP-Adresse des zweiten Nameservers.
Timeserver 1	IP-Adresse des ersten Timeservers.
Timeserver 2	IP-Adresse des zweiten Timeservers. (Vorschlag: de.ntp.pool.org)
HTTP Parent Proxy Server	IP-Adresse des übergeordneten HTTP Proxy Servers.
HTTP Parent Proxy Port	Port des übergeordneten HTTP Proxy.
HTTP Parent Proxy Login	Falls ein übergeordneter HTTP Proxy verwendet wird und dieser eine Passwort-Authentisierung verlangt, so ist hier der Benutzername einzutragen.
HTTP Parent Proxy Passwort	Falls ein übergeordneter HTTP Proxy verwendet wird und dieser eine Passwort-Authentisierung verlangt, so ist hier das Passwort einzutragen.
Mail Relay Server	Name oder IP-Adresse des Mail Relay Servers.
Mail Relay Benutzer	Benutzername für den Mail Relay Server, falls benötigt.
Mail Relay Passwort	Passwort für den Mail Relay Server, falls benötigt.
Backup-Server	IP-Adresse(n) für Backup Server, auf denen die Backups der Firewall gespeichert werden dürfen. Es können mehrere Server angelegt werden, diese sind durch Leerzeichen zu trennen.

ACHTUNG: Wenn Sie alle Einstellungen vorgenommen haben verlassen die das Menü. Speichern Sie nun alle Änderungen über den Menüpunkt *Speichern* ab und wenden Sie diese mit dem Menüpunkt *Sanft Anwenden* an. Erst nach dem Anwenden werden die neuen Einstellungen wirksam.