STATEFUL INSPECTION FIREWALL

Bintec Workshop
Version 0.9

Ziel und Zweck

Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von Bintec-Gateways ab Software-Release 7.1.4. Für neueste Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere **Release Notes** lesen – insbesondere, wenn Sie ein Software-Update zu einem höheren Release-Stand durchführen. Die aktuellsten **Release Notes** sind zu finden unter www.funkwerk-ec.com.

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Funkwerk Enterprise Communications GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie **Release Notes** für Bintec-Gateways finden Sie unter www.funkwerk-ec.com

Als Multiprotokollgateways bauen Bintec-Gateways in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. Funkwerk Enterprise Communications GmbH übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

Marken

Bintec und das Bintec-Logo sind eingetragene Warenzeichen der Funkwerk Enterprise Communications GmbH.

Erwähnte Firmen- und Produktnamen sind in der Regel Warenzeichen der entsprechenden Firmen bzw. Hersteller.

Copyright

Richtlinien und Normen

Bintec-Gateways entsprechen folgenden Richtlinien und Normen:

R&TTE-Richtlinie 1999/5/EG

CE-Zeichen für alle EU-Länder

Weitere Informationen finden Sie in den Konformitätserklärungen unter www.funkwerk-ec.com.

Wie Sie Funkwerk Enterprise Communications GmbH erreichen

Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nürnberg
Deutschland

Telefon: +49 180 300 9191 0
Fax: +49 180 300 9193 0
Internet: www.funkwerk-ec.com

Bintec France
6/8 Avenue de la Grande Lande
F-33174 Gradignan
Frankreich

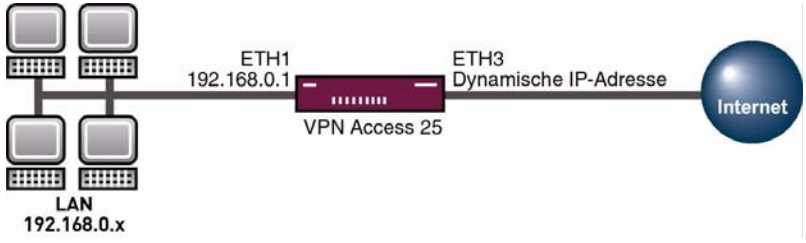
Telefon: +33 5 57 35 63 00
Fax: +33 5 56 89 14 05
Internet: www.bintec.fr

1 Einleitung

Im Folgenden wird die Konfiguration der SIF (Stateful Inspection Firewall) anhand von einem Bintec VPN Access 25 Gateway (Software Version 7.1.6 Patch 3) beschrieben.

1.1 Szenario

Den Mitarbeitern eines Unternehmens sollen nur bestimmte Dienste im Internet zur Verfügung stehen (http, https, dns). Nur der Systemadministrator soll eine Telnetverbindung zum Gateway herstellen können und der Geschäftsführer soll alle Dienste im Internet nutzen können.



Hinweis

Eine Fehlkonfiguration der Stateful Inspection Firewall kann drastische Auswirkungen auf die Funktion des Gerätes bzw. der Verbindungen haben. Auch hier gilt der bei Firewalls übliche Grundsatz: Alles was nicht explizit erlaubt ist, ist verboten. Daher ist eine genaue Planung der Filterregeln und der Filter Regelkette nötig.

1.2 Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Ein Bintec **VPN Access 25** Gateway.

- Verbindung zum Internet (siehe z.B. FAQ "Einrichtung einer xDSL Verbindung").
- Ihr LAN wird über die erste Ethernet-Schnittstelle (ETH 1) Ihres Gateways angeschlossen.
- PC einrichten (siehe Benutzerhandbuch Teil Zugang und Konfiguration).

2 Konfiguration der Stateful Inspection Firewall

2.1 Konfiguration der Alias Namen für IP-Adressen und Netzadresse

- Gehen Sie zu ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT ADDRESSES***.

```
VPN Access 25 Setup Tool                    BinTec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION][ADRESSES]: Alias Addresses       vpn25

   Alias Address List:

    Alias           IP-Address    Mask/Range        Interface
    ANY             0.0.0.0       0.0.0.0           any
    LAN_EN0-1       ------        ------            en0-1
    LAN_EN0-1-SNAP  ------        ------            en0-1-snap
    LAN_EN0-2       ------        ------            en0-2
    LAN_EN0-2-SNAP  ------        ------            en0-2-snap
    LAN_EN0-3       ------        ------            en0-3
    LAN_EN0-3-SNAP  ------        ------            en0-3-snap
    LOCAL           ------        ------            LOCAL


     ADD                 DELETE              EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return>
to edit
```

Mit ADD können Sie eigene Alias Namen hinzufügen.

- Gehen Sie zu ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT ADDRESSES*** ➜ ***ADD***.

```
VPN Access 25 Setup Tool                    BinTec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION][ADRESSES][ADD]                   vpn25

          Alias                     internes Netz

          Mode                      Address/Subnet

          IP-Address                192.168.0.0
          IP-Mask                   255.255.255.0


                    SAVE                                CANCEL
```

Folgende Felder sind relevant:

Feld	Bedeutung
Alias	Frei wählbarer Alias Name.
Mode	Verwendeter Modus.
IP-Address	IP-Adresse oder Netzadresse.
IP-Mask	Zugehörige Netzmaske.

Tabelle 2-1: Relevante Felder in ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT ADDRESSES*** ➜ ***ADD***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Tragen Sie unter ***ALIAS*** einen Namen ein, z.B. *internes Netz*.
- Wählen Sie als ***MODE*** *Address/Subnet*.
- Tragen Sie die unter ***IP-ADDRESS*** Ihre Netzadresse ein, z.B. *192.168.0.0*.
- Tragen Sie unter ***IP-MASK*** Ihre Netzmaske ein, z.B. *255.255.255.0*.
- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

Sie haben nun einen Alias Namen für das Netzwerk 192.168.0.0/24 festgelegt. Wiederholen Sie diesen Vorgang für die Konfiguration des Administrators, des Geschäftsführers und des Gateways. Die komplette Alias Liste für unser Beispiel sieht folgendermaßen aus:

- Gehen Sie zu ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT ADDRESSES***.

```
VPN Access 25 Setup Tool                    BinTec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION][ADRESSES]: Alias Addresses       vpn25

  Alias Address List:

    Alias           IP-Address    Mask/Range    Interface
    ANY             0.0.0.0       0.0.0.0       any
    LAN_EN0-1       ------        ------        en0-1
    LAN_EN0-1-SNAP  ------        ------        en0-1-snap
    LAN_EN0-2       ------        ------        en0-2
    LAN_EN0-2-SNAP  ------        ------        en0-2-snap
    LAN_EN0-3       ------        ------        en0-3
    LAN_EN0-3-SNAP  ------        ------        en0-3-snap
    LOCAL           ------        ------        LOCAL
    administrator     192.168.0.20   255.255.255.255    any
    geschaeftsfuehrer 192.168.0.100  255.255.255.255    any
    internes Netz     192.168.0.0    255.255.255.0      any
    routeradresse     192.168.0.1    255.255.255.255    any

     ADD                 DELETE              EXIT
```

2.2 Konfiguration der Alias Namen für Services

- Gehen Sie zu ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT SERVICES***.

Hinweis

Hier finden Sie eine große Anzahl bereits vorkonfigurierter Services, die für unser Beispiel ausreichen. Sie können auch eigene Services hinzufügen, z.B. *IKE*.

- Gehen Sie zu ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT SERVICES*** ➜ ***ADD.***

```
VPN Access 25 Setup Tool                    BinTec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION][SERVICES][ADD]                    vpn25

          Alias                      ike (udp:500)

          Protocol                   udp

          Port                       500     Range 1



           SAVE                                CANCEL
```

Folgende Felder sind relevant:

Feld	Bedeutung
Alias	Frei wählbarer Alias Name.
Protocol	Das vom Service verwendete Protokoll.
Port	Port bzw. Portrange, welchen der Service verwendet (das Feld muss nicht vorhanden sein wenn das Protokoll keine Ports nutzt, z.B. ESP).

Tabelle 2-2: Relevante Felder in ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT SERVICES*** ➜ ***ADD***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Tragen Sie unter ***ALIAS*** einen Namen ein, z.B. *ike (udp:500)*.
- Wählen Sie unter ***PROTOCOL*** *UDP*.
- Tragen Sie als ***PORT*** *500* ein.
- Tragen Sie als ***RANGE*** *1* ein.
- Bestätigen Sie Ihre Einträge mit **SAVE**.

Sie haben nun einen Alias Namen für Pakete, die UDP Port 500 verwenden.

2.3 Konfiguration der Filter Regeln

Nachdem die Konfiguration der Alias Namen für IP-Adressen und Services abgeschlossen ist, können Sie nun die Filter Regeln definieren.

Achtung!

Die korrekte Konfiguration der Filter Regeln und die richtige Anordnung in der Filter Regelkette sind entscheidend für die Funktion der Stateful Inspection Firewall. Eine fehlerhafte Konfiguration kann unter Umständen dazu führen, dass keine Kommunikation mit dem Internet mehr möglich ist!

- Gehen Sie zu ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT FILTERS***.

Hinweis

Beim erstmaligen Aufruf dieses Menü ist die Filter Liste noch leer.

```
VPN Access 25 Setup Tool                    BinTec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION][FILTERS]: Configuration          vpn25

   Stateful Inspection Filter List:

         Press 'u' to move Filter up or press 'd' to move Filter down.

  Pos. Source            Destination          Service            Action




     ADD                 DELETE               SAVE               CANCEL
```

Über den Menüpunkt **ADD** können Sie Filter hinzufügen.

- Gehen Sie zu ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT FILTERS*** ➜ ***ADD***.

```
VPN Access 25 Setup Tool                    BinTec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION][ADD]                              vpn25

          Source                        internes Netz
          Destination                   ANY
          Edit Addresses >

          Service                       http
          Edit Services >

          Action                        accept


           SAVE                                    CANCEL
```

Folgende Felder sind relevant:

Feld	Bedeutung
Source	Quell IP-Adresse bzw. Alias Name für diese.
Destination	Ziel IP-Adresse bzw. Alias Name für diese.
Service	Service, auf den der Filter zutreffen soll.
Action	Welche Aktion soll ausgeführt werden, wenn der Filter zutrifft.

Tabelle 2-3: Relevante Felder in ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT FILTERS*** ➜ ***ADD***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Tragen Sie unter ***SOURCE*** den Alias für Ihr internes Netzwerk ein, z.B. *internes Netz*.
- Wählen Sie unter ***DESTINATION*** *ANY*.
- Wählen Sie unter ***SERVICE*** *http*.
- Wählen Sie unter ***ACTION*** *accept*.
- Bestätigen Sie Ihre Einträge mit **SAVE**.

Sie haben nun einen Filter konfiguriert, der vom internen Netzwerk zu jeder beliebigen IP-Adresse HTTP erlaubt.

Konfigurieren Sie alle weiteren benötigten Filter analog zum vorherigen Beispiel. Die vollständige Filter Regelkette sieht wie folgt aus:

- Gehen Sie zu ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT FILTERS***.

```
VPN Access 25 Setup Tool                    BinTec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION][FILTERS]: Configuration           vpn25

   Stateful Inspection Filter List:

 Press 'u' to move Filter up or press 'd' to move Filter down.

Pos. Source            Destination     Service     Action
  1  internes Netz     ANY             http        accept
  2  internes Netz     ANY             http (SSL)  accept
  3  internes Netz     ANY             dns         accept
  4  administrator     routeradresse   telnet      accept
  5  geschaeftsfuehrer ANY             any         accept


     ADD                DELETE              SAVE                CANCEL
```

Wenn Sie die Reihenfolge der Filter ändern möchten, können Sie einen Filter markieren und ihn mit "u" nach oben bzw. mit "d" nach unten verschieben.

Sie haben nun eine Filter Regelkette konfiguriert, die alle im Szenario geforderten Punkte erfüllt.

2 Konfiguration der Stateful Inspection Firewall

3 SIF aktivieren

- Gehen Sie zu ***SECURITY*** ➜ ***STATEFUL INSPECTION***.

```
VPN Access 25 Setup Tool                    BinTec Access Networks GmbH
[SECURITY][STATEFUL INSPECTION]: Static settings                  vpn25

   Stateful Inspection Firewall global settings:

          Adminstatus    :  enable
          Local Filter   :  disable
          Full Filtering :  enable
          Logging level  :  all


          Edit Filters >
          Edit Services >
          Edit Addresses >

          Advanced settings >


             SAVE                                  CANCEL
```

Folgendes Feld ist relevant:

Feld	Bedeutung
Adminstatus	Bestimmt, ob die Stateful Inspection Firewall aktive oder inaktiv ist.

Tabelle 3-1: Relevantes Feld in ***SECURITY*** ➜ ***STATEFUL INSPECTION***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Wählen Sie unter ***ADMINSTATUS*** *enable*.
- Belassen Sie alle anderen Einstellungen.
- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

Gehen Sie zurück ins Hauptmenü und sichern Sie zum Abschluß Ihre neue Konfiguration im Flashmemory mit **EXIT** und **Save as boot configuration and exit**.

3 SIF aktivieren

4 Wichtige Hinweise

- Nach der ersten Aktivierung der Stateful Inspection Firewall werden alle aktiven Sessions erst einmal abgebrochen. Falls Sie das Gerät über Telnet konfiguriert haben wird auch Ihre Telnetsession beendet. Bei korrekter Konfiguration der SIF können Sie die Verbindung erfolgreich neu aufbauen. Ursache für dieses Verhalten: Noch aktive Sessions können von der SIF statusmäßig nicht erfasst werden.
- Am Ende der Filter Regelkette folgt ein nicht sichtbares deny. Das heisst, alle Verbindungen, die nicht vorher durch einen Filter erlaubt wurden, werden verworfen.
- Ausführliche Erläuterungen zur Stateful Inspection Firewall finden Sie zusätzlich in den Release Notes zur Version 6.2.5.

4 Wichtige Hinweise

5 Ergebnis

5.1 Test

Im folgendem Test wird dem Administrator der Zugang zum Gateway per Telnet erlaubt während ein anderer User abgelehnt wird, da keine entsprechende Regel existiert.

Geben Sie dazu in der Kommandozeile des jeweiligen PCs, folgendes ein:

```
c:\>telnet 192.168.0.1
```

Auf der Kommandozeile können Sie Debugausgaben mit dem Befehl "debug all&" anzeigen lassen. Dadurch können Sie Sessions erkennen, die von der SIF akzeptiert oder abgelehnt wurden. Geben Sie dazu folgendes in die Kommandozeile des Gateways ein:

```
vpn25:> debug all&
```

```
11:14:31 DEBUG/INET: SIF: Accept administrator[100:192.168.0.20:1277]
-> routeradresse[1:192.168.0.1:23] telnet:6
11:15:21 DEBUG/INET: SIF: No Rule ignore  192.168.0.30:1294 ->
192.168.0.1:23 Proto:6
```

5.2 Konfigurationsschritte im Überblick

Feld	Menü	Wert	Pflichtfeld
Alias	***SECURITY ➜ STATEFUL INSPECTION ➜ EDIT ADDRESSES ➜ ADD***	z.B. *internes Netz*	Ja
Mode	***SECURITY ➜ STATEFUL INSPECTION ➜ EDIT ADDRESSES ➜ ADD***	z.B. *Address/Subnet*	Ja
IP-Address	***SECURITY ➜ STATEFUL INSPECTION ➜ EDIT ADDRESSES ➜ ADD***	z.B. *192.168.0.0*	Ja
IP-Mask	***SECURITY ➜ STATEFUL INSPECTION ➜ EDIT ADDRESSES ➜ ADD***	z.B. *255.255.255.0*	Ja
Alias	***SECURITY ➜ STATEFUL INSPECTION ➜ EDIT SERVICES ➜ ADD***	z.B. *ike (udp:500)*	Ja
Protocol	***SECURITY ➜ STATEFUL INSPECTION ➜ EDIT SERVICES ➜ ADD***	z.B. *udp*	Ja
Port	***SECURITY ➜ STATEFUL INSPECTION ➜ EDIT SERVICES ➜ ADD***	*500*	Ja
Range	***SECURITY ➜ STATEFUL INSPECTION ➜ EDIT SERVICES ➜ ADD***	*1*	Ja
Source	***SECURITY ➜ STATEFUL INSPECTION ➜ EDIT FILTERS ➜ ADD***	*internes Netz*	Ja
Destination	***SECURITY ➜ STATEFUL INSPECTION ➜ EDIT FILTERS ➜ ADD***	z.B. *ANY*	Ja
Service	***SECURITY ➜ STATEFUL INSPECTION ➜ EDIT FILTERS ➜ ADD***	z.B. *http*	Ja
Action	***SECURITY ➜ STATEFUL INSPECTION ➜ EDIT FILTERS ➜ ADD***	*accept*	Ja
Adminstatus	***SECURITY ➜ STATEFUL INSPECTION***	*enable*	Ja