KB 41723: IKEIP1

IP-Tunnel mit IKEv2 einrichten auf MikroTik RouterOS

Stand	17.04.2024, 15:34:34
Version	661fcfea
Referenz-URL	https://www.internet-xs.de/kb/41723
PDF-URL	https://www.internet-xs.de/kb/Internet-XS_KB-41723-661fcfea.pdf

Zielgruppe:
Besitzer von MikroTik-Routern mit RouterOS v6.47.10+ (LTS) / 6.48.4 (Stable)

Wir betreiben verschiedene Einwahl-Server zur Bereitstellung von IP-Tunnel-Verbindungen / festen, öffentlichen IPv4-Adressen. Die Anleitungen in dieser Kategorie sind speziell abgestimmt auf diesen Server:

- Name: IKEIP1
- Hostname: ikeip1.internet-xs.de
- IP-Adresse: 212.58.69.61
- Protokoll: IKEv2 / PSK
- Client IP-Adress-Bereich: 212.58.83.0/24 (212.58.81.1 - 212.58.81.254)
- Benutzernamen-Format: ixs061-....-.....

Bitte prüfen Sie, ob Ihr IP-Tunnel-Zugang auch auf dem o.g. Server registriert ist.

Alle Arbeiten geschehen auf eigene Gefahr. Für Schäden an Soft- und Hardware sowie für Ausfälle Ihrer Infrastruktur sind Sie selbst verantwortlich. Wir können keine Unterstützung für nicht von uns getestete Szenarien, Hardware, Software und Betriebssysteme anbieten. Alle Anleitungen setzen ein Blanko- bzw. minimal konfiguriertes System voraus und sind als eine mögliche Konfigurationsvariante zu verstehen, die ggf. an Ihr lokales Umfeld und Ihre Anforderungen angepasst werden muss. Bitte beachten Sie immer die Sicherheitshinweise in der Bedienungsanleitung des Herstellers, besonders zum Betrieb von Hardware, dem Aufstellungsort und Betriebstemperaturen. Führen Sie Tests nicht in Produktivumgebungen durch. Testen Sie die Lösung ausgiebig, bevor Sie sie produktiv einsetzen. IT-Systeme sollten nur von qualifiziertem Personal konfiguriert werden. Als Administrator müssen Sie selbst abwägen, ob unsere Produkte und Dienstleistungen für Ihren Anwendungszweck und die gewünschte Verfügbarkeit geeignet sind, oder nicht. Führen Sie Änderungen nicht über eine entfernte Verbindung (Remote-Verbindung) durch. **Verwenden Sie stets sichere Passwörter, ändern Sie Standard-Passwörter umgehend ab.**

In einer PDF-Datei können Zeilenumbrüche innerhalb von Code-Blöcken vorhanden sein, da die Seitenbreite begrenzt ist. Bitte verwenden Sie für Copy & Paste im Zweifelsfall ein Editor-Programm als Zwischenritt und entfernen Sie unerwünschte Zeilenumbrüche.

Voraussetzungen

1. MikroTik Router mit RouterOS 6.49.13+ (LTS)
2. Test-Zugang oder bezahlter Zugang auf dem Einwahlserver IKEIP1 (IKEv2 / PSK)
3. Stabile Internet-Verbindung

Vorbereitung

Verbinden Sie sich per WinBox mit dem Router. Die Einrichtung per WebFig wird nicht empfohlen und ist auch nicht Teil dieser Anleitung. Eine RSC, die die meisten Einstellungen automatisch vornimmt, finden Sie am Ende der Anleitung.

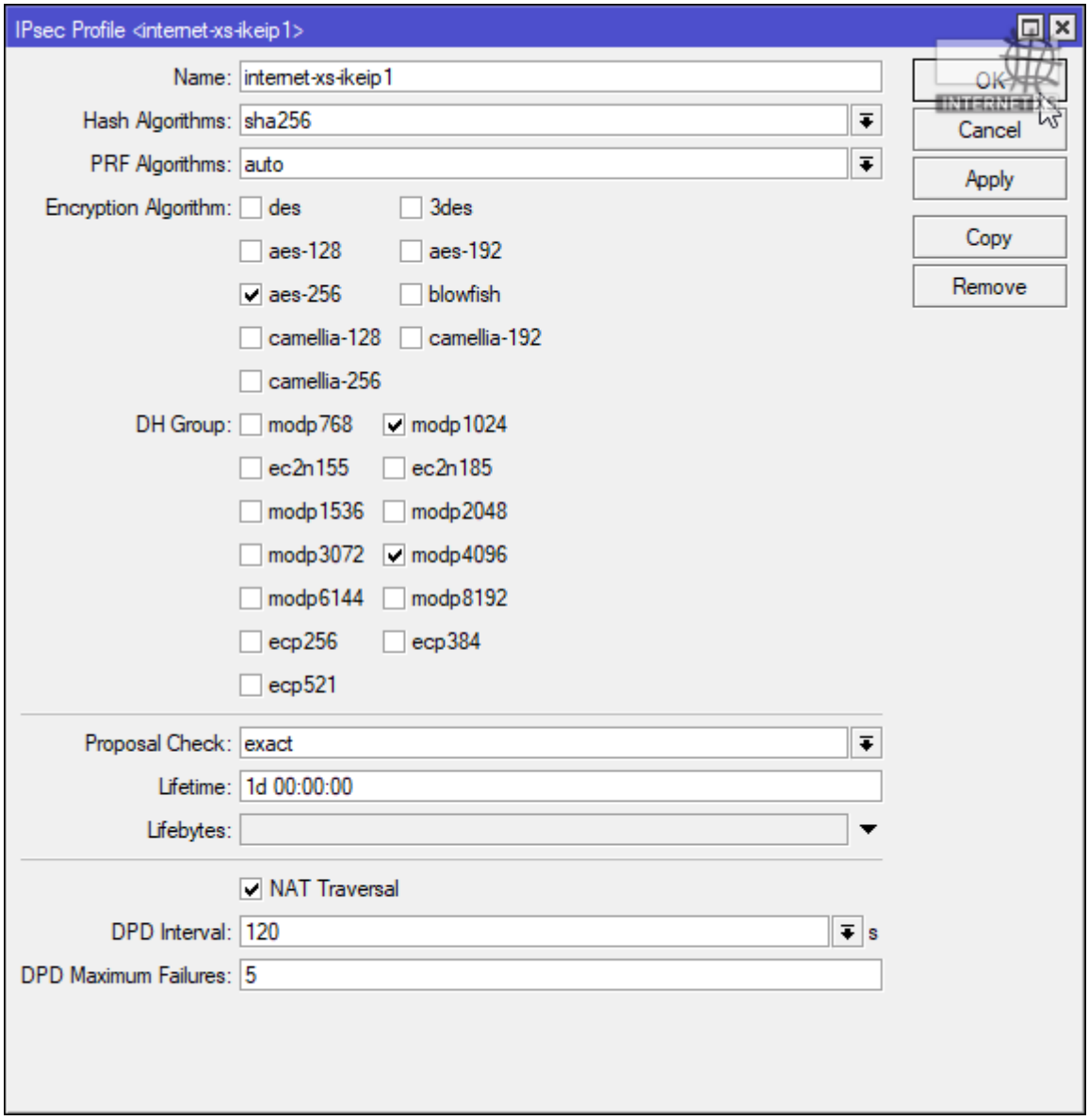
Aus praktischen Gründen gehen wir von einer Standard-Konfiguration aus. Auf individuelle Einstellungen und Anforderungen kann diese Anleitung leider keine Rücksicht nehmen.

Die Anleitung wurde an einem VDSL2-Internet-Anschluss getestet, bei dem der MikroTik-Router die PPPoE-Einwahl vornimmt. In einem kaskadierten-Router-Szenario können die Einstellungen möglicherweise abweichen.

Profile anlegen

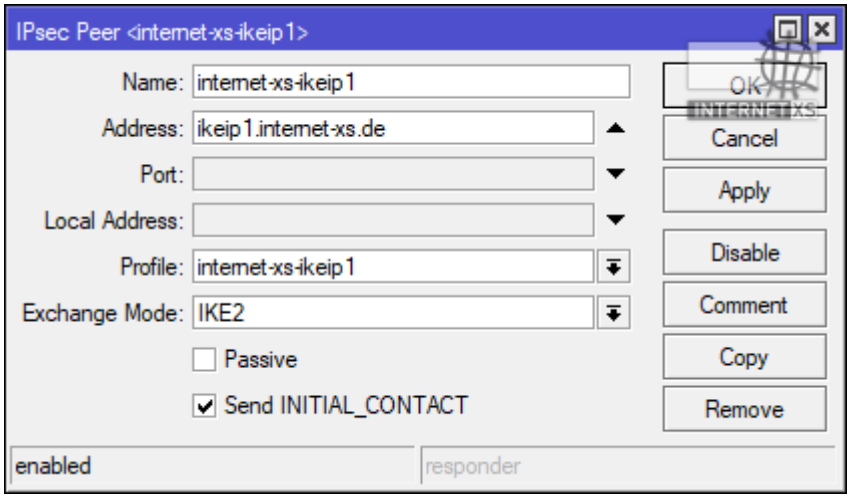
Hinweis: Die IKE-Konfiguration, auch Phase 1 genannt, wird bei MikroTik als **Profile** bezeichnet.

1. Navigieren Sie zu **IP** > **IPsec** > Reiter **Profiles**
2. Erzeugen Sie ein neues Profil durch Klick auf das blaue “+”-Symbol
3. Name: internet-xs-ikeip1
4. Hash Algorithmus: sha256
5. PRF Algorithms: auto
6. Encryption Algorithm: aes-256
7. DH Group: modp1024 und modp4096
8. Proposal Check: excat
9. Lifetime: 1d 00:00:00
10. Lifebytes: *leer*
11. NAT Traversal: aktiviert
12. DPD Interval: 120
13. DPD Maximum Failures: 5
14. Klicken Sie auf **OK**.



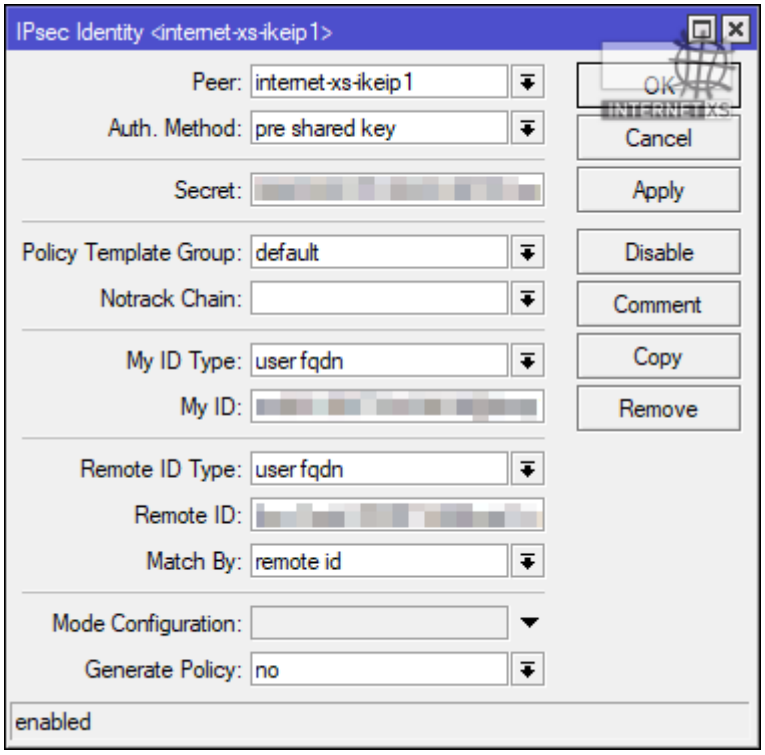
Peer anlegen

1. Navigieren Sie zu **IP** > **IPsec** > Reiter **Peers**
2. Erzeugen Sie einen neuen Peer durch Klick auf das blaue “+”-Symbol
3. Name: internet-xs-ikeip1
4. Address: ikeip1.internet-xs.de
5. Port: *leer*
6. Local Address: *leer*
7. Profile: internet-xs-ikeip1
8. Exchange Mode: IKE2
9. Passive: deaktiviert
10. Send INITIAL_CONTACT: aktiviert
11. Klicken Sie auf **OK**.



Identity anlegen

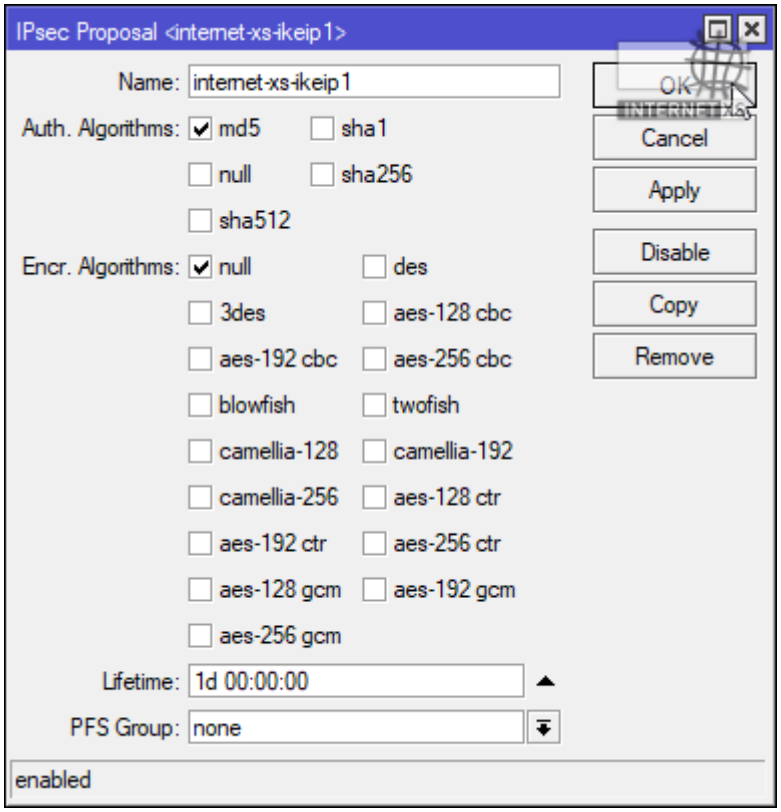
1. Navigieren Sie zu **IP** > **IPsec** > Reiter **Identities**
2. Erzeugen Sie eine neue Identity durch Klick auf das blaue “+”-Symbol
3. Peer: internet-xs-ikeip1
4. Auth. Method: pre shared key
5. Secret: *der Pre-Shared-Key / PSK wird Ihnen im Rahmen der Zustellung der Zugangsdaten mitgeteilt*
6. Policy Template Group: default
7. Notrack Chain: *leer*
8. My ID Type: user fqdn
9. My ID: *Ihre IPsec-ID wird Ihnen im Rahmen der Zustellung der Zugangsdaten mitgeteilt*
10. Remote ID Type: user fqdn
11. Remote ID: *Unsere IPsec-ID wird Ihnen im Rahmen der Zustellung der Zugangsdaten mitgeteilt*
12. Match By: remote id
13. Mode Configuration: *leer*
14. Generate Policy: no
15. Klicken Sie auf **OK**.



Proposal anlegen

Hinweis: Die IPsec-Konfiguration, auch Phase 2 genannt, wird bei MikroTik als **Proposal** bezeichnet.

1. Navigieren Sie zu **IP** > **IPsec** > Reiter **Proposals**
2. Erzeugen Sie ein neues Proposal durch Klick auf das blaue “+”-Symbol
3. Name: internet-xs-ikeip1
4. Auth. Algorithms: md5
5. Encr. Algorithms: null
6. Lifetime: 1d 00:00:00
7. PFS Group: none
8. Klicken Sie auf **OK**.

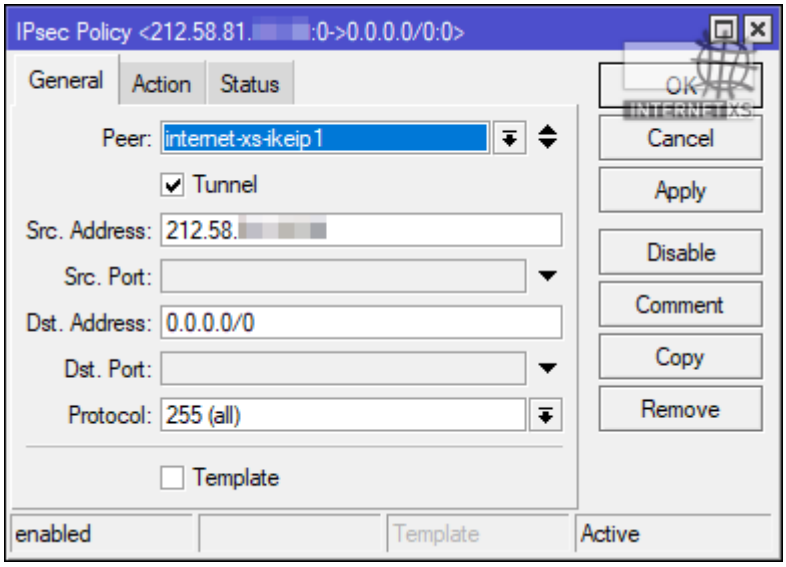


Policies anlegen

1. Navigieren Sie zu **IP** > **IPsec** > Reiter **Policies**
2. Erzeugen Sie eine neue Policy durch Klick auf das blaue “+”-Symbol

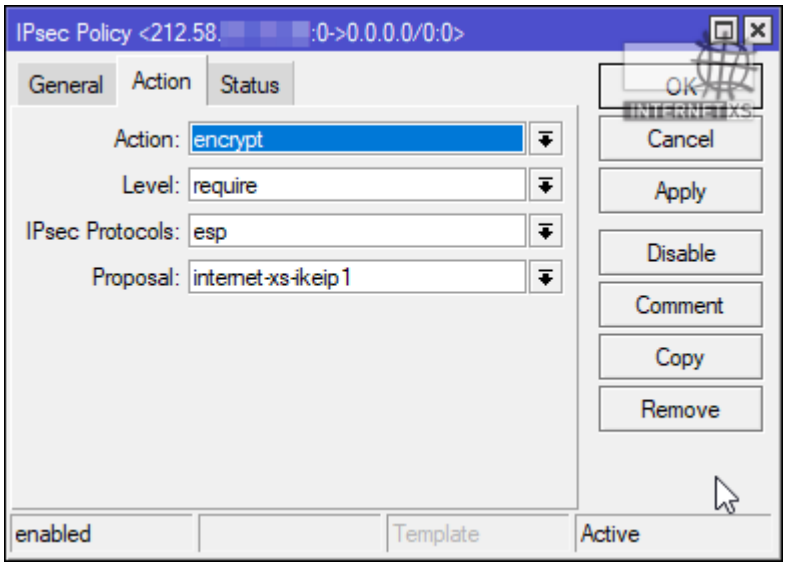
Reiter “General”

1. Peer: internet-xs-ikeip1
2. Tunnel: aktiviert
3. Src. Address: 212.58.81.X/Y *setzen Sie hier das IP-Netz ein, für das Sie Zugangsdaten erhalten haben - z.B. 212.58.81.265/28*
4. Src. Port: *leer*
5. Dst. Address: 0.0.0.0/0
6. Dst. Port: *leer*
7. Protocol: 255 (all)
8. Template: deaktiviert



Reiter “Action”

1. Action: encrypt
2. Level: require
3. IPsec Protocols: esp
4. Proposal: internet-xs-ikeip1



Klicken Sie anschließend auf **OK**.

Weitere Policies zum Auschluss von lokal anliegenden Netzen

Damit der Traffic, der zwischen lokal angelegten Netzen stattfindet nicht von der zuvor angelegten IPsec-Polocy erfasst wird, muss dieser von diesem IPsec ausgeschlossen werden.

Dieses Beispiel geht von zwei lokal angelegten Netzen aus:

- 192.168.88.0/24 : LAN
- 192.168.89.0/24 : DMZ

Dafür werden insgesamt 4 Policies für diese Kombinationen benötigt:

1. Src. Address: 192.168.88.0/24 -> Dst. Address: 212.58.81.X/Y
2. Src. Address: 212.58.81.X/Y -> Dst. Address: 192.168.88.0/24
3. Src. Address: 192.168.89.0/24 -> Dst. Address: 212.58.81.X/Y
4. Src. Address: 212.58.81.X/Y -> Dst. Address: 192.168.89.0/24

Wiederholen Sie die folgenden Schritte für alle Kombinationen - achten Sie darauf, dass die Policies zum Ausschluss von lokalen Netzen vor der Policy zum Routen des IPsec-Traffics ins Internet angelegt werden:

1. Navigieren Sie zu **IP** > **IPsec** > Reiter **Policies**
2. Erzeugen Sie eine neue Policy durch Klick auf das blaue “+”-Symbol

Reiter “General”

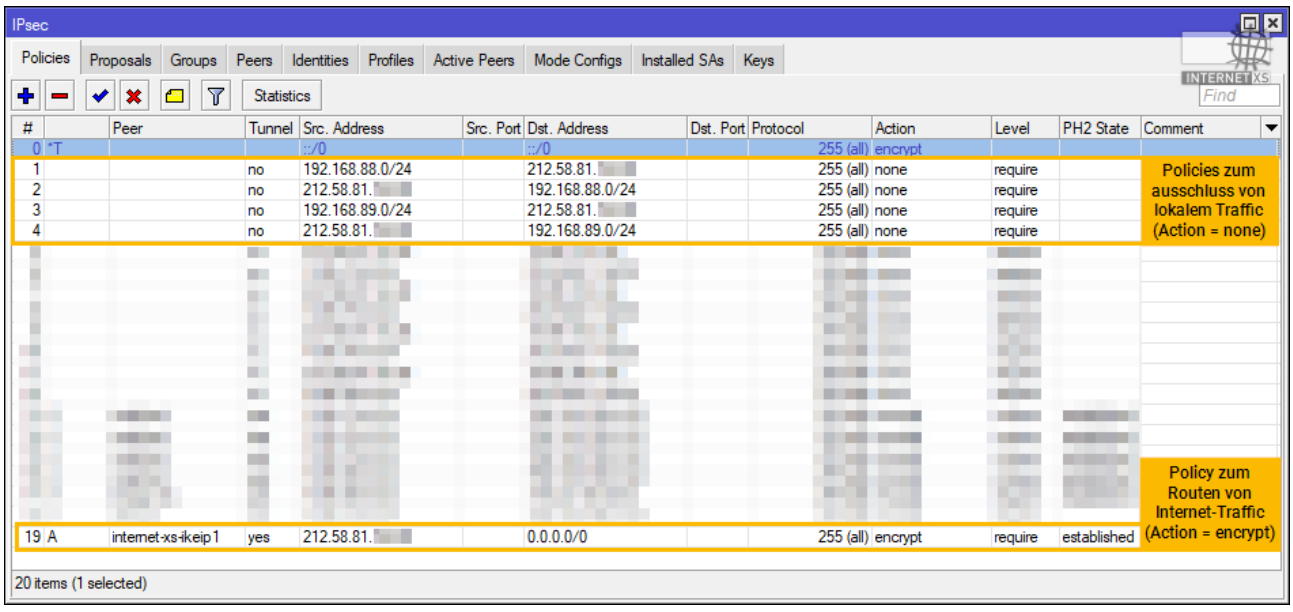
1. Peer: leer
2. Tunnel: deaktiviert
3. Src. Address: 212.58.81.X/Y *setzen Sie hier das IP-Netz ein, für das Sie Zugangsdaten erhalten haben - z.B. 212.58.81.265/28*
4. Src. Port: *leer*
5. Dst. Address: 192.168.88.0/24
6. Dst. Port: *leer*
7. Protocol: 255 (all)
8. Template: deaktiviert

Reiter “Action”

1. Action: **none**
2. Level: require
3. IPsec Protocols: esp
4. Proposal: default

Wiederholen Sie diese Schritte für alle Kombinationen.

Folgende Policies sollten dann vorhanden sein:



Bisher vorgenommene Einstellungen prüfen

Navigieren Sie zu **IP** > **IPsec**.

Reiter Active Peers

1. Spalte ID: Hier sollte unsere IPsec-ID erscheinen *unsere IPsec-ID wird Ihnen im Rahmen der Zustellung der Zugangsdaten mitgeteilt*
2. Spalte State: established
3. Local Address: *IP-Adresse Ihres Internet-Anschlusses*
4. Remote Address: 212.58.69.61
5. Dynamic Address: 0.0.0.0
6. Side: initiator
7. Uptime: > 0, z.B. 01:42:12
8. PH2 Total: > 0
9. Tx Bytes: > 0
10. Rx Bytes: > 0
11. Tx Packets: > 0
12. Rx Packts: > 0

Reiter “Installed SAs”

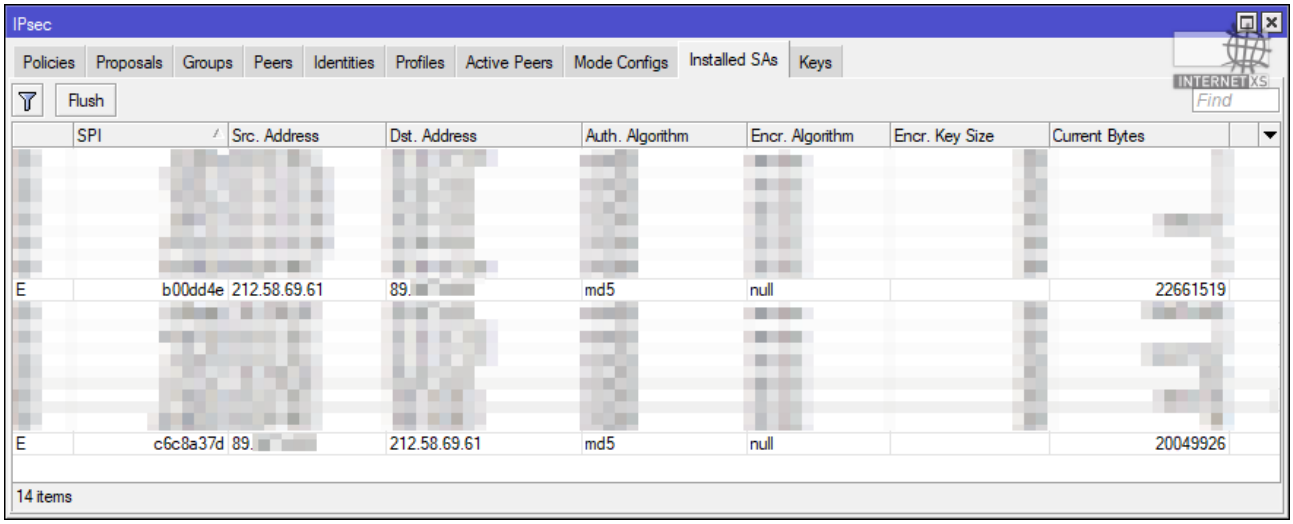
Prüfen Sie, ob diese zwei Zeilen in der Tabelle vorhanden sind (die Reihenfolge spielt keine Rolle):

1. Zeile

1. Spalte Flags: E
2. Spalte SPI: Ein 8-stelliger Hex-Wert (z.B. a1b2c3d4)
3. Spalte Src. Address: 212.58.69.61
4. Spalte Dst. Address: *IP-Adresse Ihres Internet-Anschlusses*
5. Spalte Auth. Algorithm: md5
6. Spalte Encr. Algorithm: null
7. Spalte Encr. Key Size: *leer*
8. Spalte Current Bytes: > 0

2. Zeile

1. Spalte Flags: E
2. Spalte SPI: Ein 8-stelliger Hex-Wert (z.B. d4c3b2a1)
3. Spalte Src. Address: *IP-Adresse Ihres Internet-Anschlusses*
4. Spalte Dst. Address: 212.58.69.61
5. Spalte Auth. Algorithm: md5
6. Spalte Encr. Algorithm: null
7. Spalte Encr. Key Size: *leer*
8. Spalte Current Bytes: > 0



Pseudo-Bridge anlegen

Damit Dienste, die vom MikroTik-Router selbst bereitgestellt werden, erreichbar gemacht werden können, müssen die per IKEv2 / IPsec bereitgestellten festen, öffentlichen IPv4-Adressen z.B. mittels einer Pseudo-Bridge dem Betriebssystem bekannt gemacht werden. Uns ist leider keine bessere Lösung dafür bekannt.

1. Navigieren Sie zu **Bridge**
2. Erzeugen Sie eine neue Bridge durch Klick auf das blaue “+”-Symbol

Reiter “General”

1. Name: bridge-internet-xs-ikeip1
2. ARP: disabled
3. IGMP Snooping: aktiviert (entfernt unnötige IGMP-Pakete)
4. DHCP Snooping: aktiviert (entfernt unnötige DHCP-Pakete)
5. (Add DHCP Option 82: deaktiviert)
6. Fast Forward: aktiviert

Reiter “STP”

1. Protocol Mode: none

Klicken Sie anschließend auf **OK**.

Pseudo-Bridge in Interface List “WAN” aufnehmen

Damit Traffic, der über der Pseudo-Bridge zugeordneten IPs auf dem Router eingeht (siehe nächster Schritt) von denselben Regeln erfasst wird wie Traffic, der am physikalischen Interface (z.B. VDSL) eingeht, muss die Psuedo-Bridge in die Interface List **WAN** aufgenommen werden.

1. Navigieren Sie zu **Interfaces** > Reiter **Interface List**
2. Klicken Sie auf das blaue **+**-Symbol, um einen neuen Eintrag zu erzeugen
3. List: WAN
4. Interface: bridge-internet-xs-ikeip1
5. Klicken Sie auf **OK**

Interface Addresses

Es gibt verschiedene Möglichkeiten, den Traffic, der an dem Ihnen zugeteilten IPv4-Netzwerk anliegt, an Geräte im Netzwerk zu verteilen: Bridgen (z.B. für Telefonanlagen) oder NAT (für einfache Dienste wie z.B. Web-Oberflächen, SMTP …). Bei Netzen, die groß genug sind (mind. /29), können beide Möglichkeiten parallel genutzt werden.

Beispiel: Von uns zugeteiltes Netz: 212.58.81.264**/28**

Möglichkeit 1: Transport per SNAT / DNAT

Die flexibelste Möglichkeit ist der Transport von Traffc, der an die Ihen zugeteilten festen, öffentlichen IPv4-Adressen gesendet wird, per DNAT zu einem Ziel-System (z.B. Server) bzw. Einleitung von ausgehendem Traffic (z.B. von einem Mail-Server) per SNAT in den IKEv2 / IPsec-Tunnel. **In diesem Szenario können die “Netz-Adresse” (1. Adresse, 212.58.81.264) und die “Broadcast-Adresse” (letzte Adresse, 212.58.81.279), wie Host-IPs genutzt werden.**

Die Anlage der einzelnen Adressen ist optional. Damit die Adressen für diagnosezwecke pingbar sind, jedoch empfohlen.

1. Navigieren Sie zu **IP** > **Addresses**
2. Erzeugen Sie eine neue Adresse durch Klick auf das blaue “+”-Symbol

Legen Sie alle Adressen aus Ihrem Netz (bei /29 = 8 Adressen, /28 = 16 Adressen) als **Address** an.

1. Address: 212.58.81.264/32; Network: 212.58.81.264; Interface: bridge-internet-xs-ikeip1
2. Address: 212.58.81.265/32; Network: 212.58.81.265; Interface: bridge-internet-xs-ikeip1
3. Address: 212.58.81.266/32; Network: 212.58.81.266; Interface: bridge-internet-xs-ikeip1
4. Address: 212.58.81.267/32; Network: 212.58.81.267; Interface: bridge-internet-xs-ikeip1
5. Address: 212.58.81.268/32; Network: 212.58.81.268; Interface: bridge-internet-xs-ikeip1
6. Address: 212.58.81.269/32; Network: 212.58.81.269; Interface: bridge-internet-xs-ikeip1
7. Address: 212.58.81.270/32; Network: 212.58.81.270; Interface: bridge-internet-xs-ikeip1
8. Address: 212.58.81.271/32; Network: 212.58.81.271; Interface: bridge-internet-xs-ikeip1
9. Address: 212.58.81.272/32; Network: 212.58.81.272; Interface: bridge-internet-xs-ikeip1
10. Address: 212.58.81.273/32; Network: 212.58.81.273; Interface: bridge-internet-xs-ikeip1
11. Address: 212.58.81.274/32; Network: 212.58.81.274; Interface: bridge-internet-xs-ikeip1
12. Address: 212.58.81.275/32; Network: 212.58.81.275; Interface: bridge-internet-xs-ikeip1
13. Address: 212.58.81.276/32; Network: 212.58.81.276; Interface: bridge-internet-xs-ikeip1
14. Address: 212.58.81.277/32; Network: 212.58.81.277; Interface: bridge-internet-xs-ikeip1
15. Address: 212.58.81.278/32; Network: 212.58.81.278; Interface: bridge-internet-xs-ikeip1
16. Address: 212.58.81.279/32; Network: 212.58.81.279; Interface: bridge-internet-xs-ikeip1

Ab jetzt sollten die einzelnen IPs aus dem Internet pingbar sein (vorausgesetzt es gibt keine Firewall-Filter-input-Regel, die dies verhindert).

DNAT konfigurieren

Beispiel: 212.58.81.272 Port 443 (HTTPS) soll an die DMZ-IP-Adresse 192.168.89.15 Port 443 weitergeleitet werden.

1. Navigieren Sie zu **IP** > **Firewall** > Reiter **NAT**
2. Erzeugen Sie eine neue Regel durch Klicken auf das blaue “+”-Symbol

3. Reiter **General**:
4. Chain: dstnat
5. Dst. Address: 212.58.81.272
6. Protocol: 6 (tcp)
7. Dst. Port: 443
8. Reiter **Action**:
9. Action: dst-nat
10. To Addresses: 192.168.89.15
11. Klicken Sie auf **OK**

Wiederholen Sie diese Schritte für alle Ports, die weitergeleitet werden sollen.

SNAT konfigurieren

Beispiel: Jeglicher Traffic, der von der DMZ-IP-Adresse 192.168.89.17 ins Internet geht, soll mit der IP-Adresse 212.58.81.277 versehen werden.

1. Navigieren Sie zu **IP** > **Firewall** > Reiter **NAT**
2. Erzeugen Sie eine neue Regel durch Klicken auf das blaue “+”-Symbol
3. Reiter **General**:
4. Chain: srcnat
5. Src. Address: 192.168.89.17
6. Reiter **Action**:
7. Action: src-nat
8. To Addresses: 212.58.81.277
9. Klicken Sie auf **OK**

Filter Rules

Forward-Traffic, d.h. Traffic zwischen verschiedenen Netzen, sollte in einem vernünftig konfigurierten Firewall-Router aus Sicherheitsgründen grundsätzlich blockiert werden. Um Traffic, der per SNAT / DNAT explizit zwischen zwei Netzen (= Internet und DMZ bzw. DMZ und Internet) vermittelt wurde, auch auf der “Filter Rules”-Ebene zu erlauben, kann eine einzige Regel angelegt werden:

1. Navigieren Sie zu **IP** > **Firewall** > Reiter **Filter Rules**
2. Erzeugen Sie eine neue Regel durch Klicken auf das blaue “+”-Symbol
3. Reiter **General**:
4. Chain: forward
5. Connection NAT State: dstnat
6. Reiter **Action**:
7. Action: accept
8. Klicken Sie auf **OK**

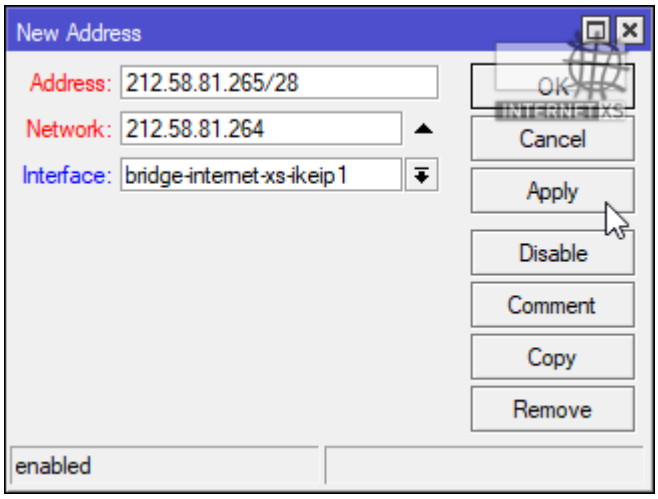
Alternativ können Sie für alle SNATs / DNATs einzelne Regeln im “forward”-Chain anlegen.

Möglichkeit 2: Bridgen der IP-Adressen auf angeschlossene Geräte / Server

Die über den IKEv2 / IPsec bereitgestellten festen, öffentlichen IPv4-Adressen können direkt auf angeschlossenen Servern / beliebigen Geräten genutzt werden.

1. Navigieren Sie zu **IP** > **Addresses**
2. Legen Sie ein neues Netz durch Klick auf das blaue “+”-Symbol an

3. Address: 212.58.81.265**/28** (= 1. Host-Adresse aus dem Netz 212.58.81.264/28)
4. Network: 212.58.81.264
5. Interface: Pseudo-Bridge (bridge-internet-xs-ikeip1)



Sie können jetzt auf angeschlossenen Geräten / Servern diese IP-Konfiguration vornehmen:

- IP-Adresse: 212.58.81.266 oder 212.58.81.267 oder 212.58.81.268 oder 212.58.81.269 oder 212.58.81.270 … bis 212.58.81.278
- Subnetzmaske: 255.255.255.240 (= /28)
- Gateway: 212.58.81.265 (= 1. Host-Adresse - IP-Adresse des MikroTik-Routers)
- Netzadresse: 212.58.81.264
- Broadcast-Adresse: 212.58.81.279

Möglichkeit 3: Beide Möglichkeiten nutzen

Wenn Sie über ein Netz verfügen, das groß genug ist, können Sie beide Möglichkeiten nutzen. Es wird jedoch empfohlen, mindestens ein /28-Netz (16 IPs) zu verwenden (mind. /29-Netz erforderlich).

Teilnetz für Möglichkeit 1: 212.58.81.264**/29** - Adressen einzeln (= /32 / 255.255.255.255) für alle 8 IPs in diesem Netz anlegen:

- Address: 212.58.81.264/32; Network: 212.58.81.264; Interface: bridge-internet-xs-ikeip1
- Address: 212.58.81.265/32; Network: 212.58.81.265; Interface: bridge-internet-xs-ikeip1
- Address: 212.58.81.266/32; Network: 212.58.81.266; Interface: bridge-internet-xs-ikeip1
- Address: 212.58.81.267/32; Network: 212.58.81.267; Interface: bridge-internet-xs-ikeip1
- Address: 212.58.81.268/32; Network: 212.58.81.268; Interface: bridge-internet-xs-ikeip1
- Address: 212.58.81.269/32; Network: 212.58.81.269; Interface: bridge-internet-xs-ikeip1
- Address: 212.58.81.270/32; Network: 212.58.81.270; Interface: bridge-internet-xs-ikeip1
- Address: 212.58.81.271/32; Network: 212.58.81.271; Interface: bridge-internet-xs-ikeip1

Teilnetz für Möglichkeit 2: 212.58.81.272**/29** - Addresse für für das /29-Netz anlegen:

- 212.58.81.273/255.255.255.248

Für angeschlossene Geräte / Server ergibt sich darausfolgende IP-Konfiguration:

- IP-Adresse: z.B. 212.58.81.274 oder 212.58.81.275 oder 212.58.81.276 oder 212.58.81.277 oder 212.58.81.278
- Subnetzmaske: 255.255.255.248

- Gateway: 212.58.81.273
- Netzadresse: 212.58.81.272
- Broadcast-Adresse: 212.58.81.279

Firewall-Regeln

Raw-Tabelle

Falls Sie Traffic in der Raw-Tabelle filtern, ist möglicherweise das bedingungslose Akzeptieren von IPsec-Traffic erforderlich:

1. Navigieren Sie zu **IP** > **Firewall** > **Raw**
2. Erzeugen Sie ein neue Regel durch Klick auf das blaue “+”-Symbol
3. Reiter **General** - Chain: prerouting
4. Reiter **Advanced** - IPsec Policy: in : ipsec
5. Reiter **Action** - Action: accept

Sie können diese Regel natürlich auch beliebig weiter einschränken.

Klicken Sie anschließend auf **OK**.

Abschluss

Die Einrichtung eines IKEv2 / IPsec-Tunnels zum Transport von festen, öffentlichen IPv4-Adressen ist damit abgeschlossen. Bitte testen Sie die Firewall-Regeln sorgfältig, um Sicherheitslücken zu vermeiden.

Impressum

Verantwortlich für die Inhalte in diesem Dokument:

Internet XS Service GmbH
Internetagentur
Heßbrühlstr. 15
70565 Stuttgart

Telefon: 07 11/78 19 41 - 0
Telefax: 07 11/78 19 41 -79
E-Mail: info@internet-xs.de
Internet: www.internet-xs.de

Geschäftsführer: Helmut Drodofsky
Registergericht: Amtsgericht Stuttgart
Registernummer: HRB 21091
UST.IdNr.: DE 190582774

Alle Preise, sofern nicht ausdrücklich anders gekennzeichnet, inkl. gesetzlich geldender deutscher MwSt.

Angebote, sofern nicht ausdrücklich anders gekennzeichnet, gültig bis 4 Wochen nach Zusendung / Abruf.

