KB 36654: IKEIP1

Technische Spezifikation ikeip1.internet-xs.de

Stand	27.09.2022, 12:01:02
Version	6332c9de
Referenz-URL	https://www.internet-xs.de/kb/36654
PDF-URL	https://www.internet-xs.de/kb/Internet-XS_KB-36654-6332c9de.pdf

Inhalt

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.

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.

Technische Spezifikation

Feld	Wert
Tunnel-Protokoll	IKEv2 / IPSec mit PSK
Netzwerk-Protokoll	4500/UDP (IPSec)
Host	ikeip1.internet-xs.de / 212.58.69.61
Benutzer-Authentifizierung	IPSec-ID / PSK
Verschlüsselung	IKEv2: Ja, IPSec: Nein (optional Verschlüsselung möglich, wenn auch nicht sinnvoll)
Client-IP-Bereich	212.58.81.0/24 (212.58.81.1 - 212.58.81.254)
Benutzernamen-Formate	ixs061-1234-a1b2c3d4
IPSec-ID	wird im Rahmen der Zuteilung des IP-Tunnels mitgeteilt
PSK	wird im Rahmen der Zuteilung des IP-Tunnels mitgeteilt
TCP-MSS	1410 (wird serverseitig eingestellt)

Generische Konfigurationsanleitung

Konfigurationsoption	Alternative Bezeichnungen	Wert
Modus	Protokoll, Protocol	IKEv2 mit PSK
Right IP	Server-IP, Gateway IP, Peer IP	212.58.69.61
PSK	Pre-Shared-Key, Vorinstallierter Schlüssel	Wird im Rahmen der Zuteilung der Zugangsdaten mitgeteilt
Left ID	Lokale ID, My ID	Wird im Rahmen der Zuteilung der Zugangsdaten mitgeteilt
Right ID	Entfernte ID, Peer ID	Wird im Rahmen der Zuteilung der Zugangsdaten mitgeteilt
Left Subnet	Lokales Subnetz, Local Subnet, My Subnet	Wird im Rahmen der Zuteilung der Zugangsdaten mitgeteilt
Right Subnet	Entferntes Subnetz, Remote Subnet, Peer Subnet	0.0.0.0/0
Phase 1 Key Lifetime	IKE Key Lifetime	86400 Sekunden
Phase 1 DH	IKE DH-Gruppe, Phase 1 Schlüsselgruppe	6 / 4096
Phase 1 Encryption	IKE Verschlüsselung	AES256
Phase 1 Authentication	IKE Authentifizierung, Hash Algorithmus	SHA256
Phase 2 PFS Group	IPsec DH-Gruppe, Phase 2 Schlüsselgruppe, ESP	NULL oder NONE oder KEINE
Phase 2 Key Lifetime	IPsec / ESP Key Lifetime	86400 Sekunden
Phase 2 Encryption	IPsec / ESP Verschlüsselung	NULL oder NONE oder KEINE
Phase 2 Authentication	IPsec / ESP Authentifizierung, Hash Algorithmus	MD5
DPD Timeout	Dead Peer Detection Zeitüberschreitung	300 Sekunden
DPD Delay	Dead Peer Detection Verzögerung	120 Sekunden

Terminologie

IPsec ist nicht ausschließlich ein Client-Server-Modell - beide Seiten können theoretisch beide Funktionen einnehmen. Deshalb haben sich diese Bezeichnungen für die jeweilige Seite etabliert:

- Eigene Seite: “Left”, “Local”, “My”
- Entfernte Seite: “Right”, “Remote”, “Peer”

Aus Sicht der aufbauenden Seite (Ihre Seite) ist die Gegenstelle (unsere Seite) ein **Responder**, die aufbauendende Seite (Ihre Seite) ein **Initiator**. Je nach Konfiguration können die Rollen jederzeit wechseln, wobei unsere Seite ein “Respond Only”-Gateway ist, d.h. nicht selbst aktiv Verbindungen zur Kundenseite aufbaut und deshalb nie **Initiator** sein kann, nur **Responder**.

Right Subnet 0.0.0.0/0

In IPsec definieren beide Gegenstellen, welche Datenpakete überhaupt innerhalb des Tunnels von welcher Seite akzeptiert werden (sog. “Traffic Selector”).

- Wir definieren, dass wir Datenpakete aus Ihrem Tunnel mit IPs aus dem Ihnen zugeteilten Netz akzeptieren (“Left Subnet” / “Local Subnet”).
- Sie definieren, dass Sie Datenpakete aus dem Tunnel mit einer beliebigen Absender-IP-Adresse (= 0.0.0.0/0) akzeptieren (“Right Subnet” / “Remote Subnet”).

Diese Einstellung hat zunächst keinen Einfluss auf das Routing im Betriebssystem, da IPsec als zusätzliche Schicht außerhalb des regulären Routings fungiert weil IPsec (anders als bei OpenVPN, L2TP, PPTP, Wireguard) keine virtuellen Interfaces kennt (abgesehen von VTI, das jedoch herstellerspezifisch ist und deshalb nicht von uns unterstützt wird), auf die überhaupt geroutet werden könnte.

Es sollte also auf keinen Fall eine neue “Default Route” in der Routing-Tabelle des Betriebssystems erscheinen. Falls dies der Fall sein sollte, verwenden Sie eine herstellerspezifische Funktion (wie bspw. “Bind Tunnel on Local Interface”, “ARP Proxy” oder “VTI”), die für dieses Szenario nicht aktiviert werden sollte oder die IPsec-Implementierung ist fehlerhaft.

Wie gelangt Traffic von meiner Seite aus in den Tunnel?

Wenn Sie Datenpakete in den Tunnel schicken möchten, müssen Sie entweder mittels

- SNAT
- per “Bridging” auf bspw. eine VM (z.B. für Telefonanlagen) (mind. /30-Netz erforderlich)
- “Additional Interface Address” (die genaue Bezeichnung variiert von Hersteller zu Hersteller / Betriebssystem zu Betriebssystem)

Datenpakete generieren, die als Absender-IP-Adresse eine der Ihrem Netz (“Left Subnet” / “Local Subnet”) zugeteilten IPs verwenden. Die IPsec-Implementierung auf Ihrer Seite des Tunnels sollte diese Pakete dann automatisch in den Tunnel schicken.

Verschlüsselung in Phase 2

Die Verschlüsselung von Phase 2 ist absichtlich ausgeschaltet um die maximale Performance zu erreichen und nicht ein falsches Gefühl von Sicherheit zu erwecken - Wenn Sie Dienste über die feste IP bereitstellen (Webseiten, Mailserver usw.), sollten diese ihrerseits “wie immer” mit bspw. SSL/HTTPS usw. verschlüsselt sein, da alles andere keine E2E-Verschlüsselung wäre da der Tunnel mit der festen IP nur zwischen Ihrem Endpunkt und unserem Server existiert, nicht jedoch zwischen bspw. einem zugreifenden Nutzer aus dem Internet und unserem Server.

Abgesehen davon sind Daten, die aus diesem Tunnel kommen, immer als unsicher zu betrachten da die Quelle eine beliebige im Internet ist und nicht - wie normalerweise bei einer IPSec Site-2-Site-Verbindung - eine vertrauenswürdige Gegenstelle wie bspw. eine Unternehmenszentrale / Filiale o.Ä.

Bitte achten Sie deshalb besonders auf eine sichere Firewall-Konfiguration.

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.

