

Public

Check list

Remote Access over Internet via

Site to site IPsec tunnel

author(s) : R. Niklowitz

document number : CCT-FFF-0001

version : 6.2

status : Final

source : Atos Unify

document date : 5th September 2022­

­

­

number of pages : 13

owner : R.Niklowitz

© Copyright 2021, Unify Communication and Collaboration Services GmbH All rights reserved. Reproduction in whole or in part is prohibited without the prior written consent of the copyright owner. For any questions or remarks on this document, please contact Atos Unify, +49 89 7007 23257.

Content

[1 Introduction 4](#_Toc76474583)

[2 Installation and Configuration 5](#_Toc76474584)

[2.1 General contact data 5](#_Toc76474585)

[2.1.1 Your data 5](#_Toc76474586)

[2.2 IPsec tunnel 6](#_Toc76474587)

[2.2.1 Overview 6](#_Toc76474588)

[2.2.2 Tunnel data 6](#_Toc76474589)

[2.2.3 Encryption Domain (interesting traffic)- Seen From Your Side 9](#_Toc76474590)

[2.3 Device list 10](#_Toc76474591)

[2.4 Firewall port list 12](#_Toc76474592)

[3 Appendix A 13](#_Toc76474593)

List of changes

| version | Date | Description | Author(s) |
| --- | --- | --- | --- |
| V1.0 | 12/04/2015 | 1st release | R. Niklowitz,  M. Knerrich |
| V4.12 | 25/06/2019 | General revision, added Options with higher security | R. Niklowitz |
| V5.0 | 02/12/2020 | Atos template requirements applied, general yearly review, SNow requirements revised, Port list revision updates | D.Tropolinova. B.Beshkov, R. Niklowitz |
| V6.0 | 26/05/2021 | Add IKE V2 standard and security parameters as BSI recommends | R.Niklowitz |
| V6.1 | 06/07/21 | Minor corrections and add lifetime | R.Niklowitz |

# Introduction

Remote access to customer systems over Internet via an IPsec tunnel with our “Remote Service Platform” (RSP) is an essential component of a fast and secure remote infrastructure.

This checklist describes all necessary data required in a network provided by the customer for the installation and configuration of an access. These data must be given before requesting remote access.

*Explanation of symbols and signs:*

|  |  |
| --- | --- |
| Symbol | Supplied / provided by: |
| C | Customer |
| V/E | Sales / Engineering |
| S | Service in cooperation with Atos Unify onboarding team |
| S/C | Service in cooperation with customer |

*If you have any questions, please contact:*

|  |  |  |
| --- | --- | --- |
| V/E | Name |  |
| V/E | Zip code, location |  |
| V/E | Street |  |
| V/E | Phone number |  |
| V/E | Email |  |

# Installation and Configuration

## General contact data

### Your data

##### General:

|  |  |  |
| --- | --- | --- |
| C | Company name |  |
| S/C | Contract number |  |
| C | Road, number |  |
| C | ZIP code, City |  |
| C | Country |  |

##### Network administration and /or technical contact partner:

|  |  |  |
| --- | --- | --- |
| C | Name |  |
| C | Phone number |  |
| C | Email |  |

##### Network - Helpdesk (if available):

|  |  |  |  |
| --- | --- | --- | --- |
| C | Name (if this is a person) |  |  |
| C | Phone number |  |  |
| C | Email |  |  |
| C | Business hours Mo – Fr |  |  |
| C | Business hours Sa + Su |  |  |
| C | Time zone |  |  |

##### Emergency contact (if available):

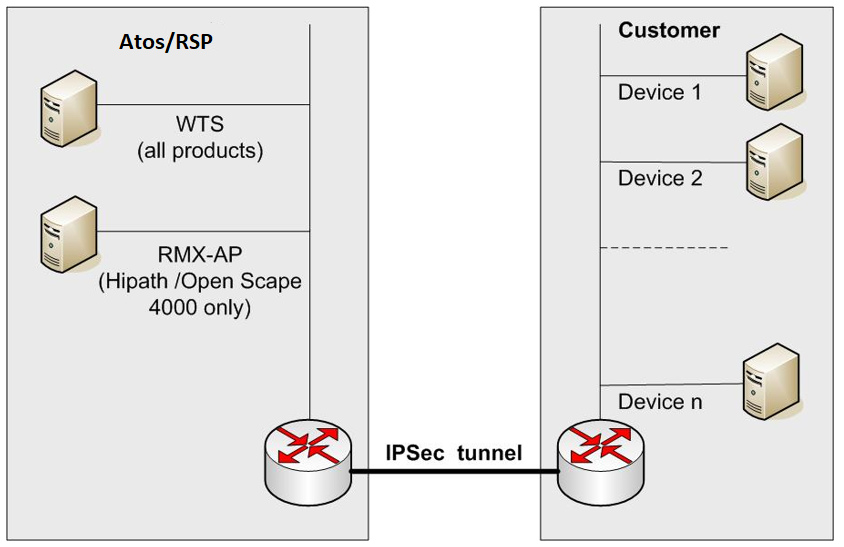
|  |  |  |
| --- | --- | --- |
| C | Customer network helpdesk name (if this is a person) |  |
| C | Phone number |  |
| C | Email |  |
| C | Remarks (e.g. availability other than 24 hours / 7 days) |  |

##### Atos Unify contact data:

|  |  |  |
| --- | --- | --- |
|  | Name | RSP On-Boarding |
|  | Phone number | +49 (89) 7007 16000 |
|  | Email | ccs\_rsp-emea@atos.net |

## IPsec tunnel

### Overview



### Tunnel data

##### General:

|  |  |  |  |
| --- | --- | --- | --- |
| S/C | Is it possible to use a Site-to-Site-IPsec - tunnel? (LAN-to-LAN - access) | ( ) **YES,** continue with next line | ( ) **NO**, then remote access over IPsec is NOT possible. |
| S/C | It’s possible to have access to remote hosts the whole time? | ( ) **YES,** then continue with “Phase I” | ( ) **NO**, then please describe briefly the necessary procedure (see below) |

Brief description for the necessary procedure to open the access (e.g.: special authentication):

|  |
| --- |
|  |

( ) Use Of IKE V2

Please notify:

* vendors strongly recommend using the same parameters in Phase 2 as in Phase 1. Please choose the Phase 2 parameters accordingly
* the specified parameter sets correspond to the recommendations of the BSI (German Federal Office for Information Security)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Your tunnel endpoint (Customer) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
|  | Tunnel endpoint Atos-Unify RSP | 188.64.18.4 | | |
|  | Parameter sets: | 1st: ( ) | 2nd: ( ) | Legacy: ( ) |
|  | Phase I (ISAKMP) |  | | |
|  | Authentication mode | Pre-shared Key | | |
|  | Encryption type | AES 256 CBC | AES 256 CBC  AES 128 CBC | AES 256 CBC |
|  | Integrity | SHA 512 SHA 384 SHA 256 | SHA 256 | SHA 256 |
|  | DH group | Group 21 | Group 20 Group 19 | Group 16  Group 14 |
|  | Lifetime | 28800s ( ) or others:\_\_\_\_\_\_\_\_\_\_\_ | | |
|  | Phase II (IPsec) |  | | |
|  | Encryption type | ( ) AES 256 CBC  ( ) AES 128 CBC | | |
|  | Integrity | ( ) SHA 512  ( ) SHA 384  ( ) SHA 256 | | |
|  | PFS | ( ) Group 21  ( ) Group 20  ( ) Group 19  ( ) Group 16  ( ) Group 14 | | |
|  | Lifetime | 3600s ( ) or others:\_\_\_\_\_\_\_\_\_\_\_ | | |

( ) Use Of IKE V1

Please notify:

* vendors recommend strongly using the same parameters in Phase 2 as in Phase 1. Please choose the Phase 2 parameters accordingly

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Ihr Tunnelendpunkt (Kunde) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
|  | Tunnelendpunkt Atos-Unify RSP | 188.64.18.11 | | |
|  | Proposal: | 1st: ( ) | 2nd: ( ) | 3rd: ( ) |
|  | Phase I (ISAKMP) |  | | |
|  | Authentication mode | Pre-shared Key | | |
|  | Encryption type | AES 256 CBC | AES 256 CBC | AES 256 CBC |
|  | Integrity | SHA 512 | SHA 256 | SHA 256 |
|  | DH group | Group 21 | Group 20 | Group 16 or 14 |
|  | Lifetime | 28800 sec | | |
|  | Phase II (IPsec) |  | | |
|  | Encryption type | ( ) AES 256 CBC | | |
|  | Integrity | ( ) SHA 512  ( ) SHA 256 | | |
|  | PFS | ( ) Group 21  ( ) Group 20  ( ) Group 16  ( ) Group 14 | | |
|  | Lifetime | 3600s ( ) or others:\_\_\_\_\_\_\_\_\_\_\_ | | |

##### Preshared Key:

|  |  |  |
| --- | --- | --- |
| S/C | Pre shared secret exchange  procedure:  (maximum 127 characters, “**?**“is not allowed) | ( ) Phone call  ( ) SMS  ( ) or other, please specify (for example a bitmap in mail…) |

### Encryption Domain (interesting traffic)- Seen From Your Side

##### Hardware on your side:

|  |  |  |
| --- | --- | --- |
| S/C | VPN Gateway manufacturer: |  |
| S/C | VPN Gateway product / version: |  |

##### Local IP addresses (Source addresses – your devices):

|  |  |  |  |
| --- | --- | --- | --- |
| S/C | Do you use public IP addresses? | **( ) YES,** then please specify the network(s) in the lines below. You don’t need to fill in the next line. | **( ) NO,** then continue with next line. |
| S/C | Could you add the Encryption Domain host by host?  Encryption Domain added all hosts separately is preferred rather than by networks. If networks are required, please use small networks (no more than 32 hosts or /28). | **( ) YES,** the Encryption Domain has to contain all hosts separately.  Hosts see point 2.3 | **( ) NO,** the please specify the network(s) in the lines below this table |

Please specify the networks:

|  |
| --- |
|  |

##### Remote IP address (Destination address - RSP address):

|  |  |  |  |
| --- | --- | --- | --- |
| S | All RSP server are reachable by the following single IP address: | 188.64.18.28 | |
| S/C | Are you able to route the IP address above in the IPsec tunnel? | **( ) YES,** then please configure 188.64.18.28 / 32 (255.255.255.255) | **( ) NO,** then please define in the field below an address you are able to route. Atos/Unify will be translate this address in the native RSP IP address. |

Please specify the IP addresses to translate to:

|  |
| --- |
|  |

## Device list

Short description:

*CIdataextID(CMDB)/ External UID (SNow)* (\*2) is a unique ID to identify devices in our Customer database (CMDB) or ServiceNow (CIDB). It will be provided by Atos Unify.

*Device NAT address* (\*5) is only necessary if it’s not possible to access the device via its real address.

*Device IP address* (\*6) is the real address of a device in your network.

If it’s necessary to address more than 15 devices please extend this table.

| No. | CI ID/EUID | Device serial number | Product name and version | NAT address (if NAT necessary) | Device IP address | Username | Password |
| --- | --- | --- | --- | --- | --- | --- | --- |
| \* | \*2 (A/E) | \*3 (S/C) | \*4 (S/C) | \*5 (S/C) | \*6 (S/C) | \*7 (S/C) | \*8(S/C) |
| 1 |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |  |
| 8 |  |  |  |  |  |  |  |
| 9 |  |  |  |  |  |  |  |
| 10 |  |  |  |  |  |  |  |
| 11 |  |  |  |  |  |  |  |
| 12 |  |  |  |  |  |  |  |
| 13 |  |  |  |  |  |  |  |
| 14 |  |  |  |  |  |  |  |
| 15 |  |  |  |  |  |  |  |

## Firewall port list

Please refer this embedded list to release all necessary ports in a firewall on your network. Please note, this is a generic list that contains all possible products and ports, despite it will be used in your configuration or not.

We could also provide a port list for you considering your configuration.



# Appendix A

| Abbreviations and technical terms | Explanation |
| --- | --- |
| LAN | Local Area Network |
| SIRA | Secured Infrastructure for Remote Access database and frontend used by Atos Unify for remote access |
| VPN | Virtual Private Network |
| WTS | Windows Terminal Server |
| RSP | Remote Service Platform contains all hard and software components including SIRA used by Atos Unify for remote access |
| Snow | Atos ServiceNow toolset |