Roadmap to Securing Enterprise Extender Traffic over an APPN Global Connection Network

Share Conference
Heinz Klümper (Fl) & Matthias Burkhard (IBM)
February 03 - 08, 2013, San Francisco
Personal Introduction

Heinz Klümper
(Finanz Informatik)

phone: +49 (0) 251 288-33697

email: heinz.kluemper@f-i.de
Agenda

1. The IT Service Provider Finanz Informatik
2. Initial situation and objectives
3. Overview of changes
4. TCP/IP customizations
5. VTAM customizations
6. Paths in the APPN network
7. Customization for data encryption
8. The result
9. Gained experiences
10. Troubleshooting and solved problems
The company serves a large part of the German retail banking market

**Finanz Informatik – Company**

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenue (in mill. €) (2011)</td>
<td>1,453</td>
</tr>
<tr>
<td>with saving banks</td>
<td>1,004</td>
</tr>
<tr>
<td>with state banks</td>
<td>229</td>
</tr>
<tr>
<td>Employees (full-time equivalents)</td>
<td>4,975</td>
</tr>
</tbody>
</table>

**Customers**

<table>
<thead>
<tr>
<th>Category</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Savings banks</td>
<td>423</td>
</tr>
<tr>
<td>State banks + DekaBank</td>
<td>9</td>
</tr>
<tr>
<td>State home loan banks</td>
<td>10</td>
</tr>
<tr>
<td>Accumulated balance sheet of supported</td>
<td>1,046</td>
</tr>
<tr>
<td>savings banks (in bill. €) (2011)</td>
<td></td>
</tr>
</tbody>
</table>

**Market Share (Savings)¹)**

- Savings Banks Financial Group: 50.2%
- Credit Unions: 20.7%
- Private Banks, other: 29.1%

¹) Sources: DSGV (12/31/2011); German Federal Bank, Others.
Significant scale can be achieved through bundling volume IT services

**Supported financial institutions**

| Supported branches of supported savings banks | 15,250 |
| Bank-specific employees of supported savings banks (2010) | 192,301 |

**Processing volumes**

| Booked entries per annum (in bill.) | 11 |
| Supported accounts (in mill.) | 127 |

**Devices**

| ATMs | 24,029 |
| Statement printers | 15,812 |
| Other self-service terminals | 13,633 |
| MIPS (Mainframe) | 386,950 |
| DASD Terabyte (Mainframe) | 2,836 |
| Windows-Sever | 11,904 |
| UNIX-Server | 2,564 |
# Agenda

1. The IT Service Provider Finanz Informatik

2. Initial situation and objectives

3. Overview of changes

4. TCP/IP customizations

5. VTAM customizations

6. Paths in the APPN network

7. Customization for data encryption

8. The result

9. Gained experiences

10. Troubleshooting and solved problems
Initial situation

- APPN communication links between 12 NetIDs
- No direct APPN communication (CrossNetid) between END NODEs
- Within the APPN area no „End to End“ encryption

Objectives

- Establish a direct communication between all APPN NODE types with the option to encrypt the data
Initial situation and objectives (2/2)

Solution

Establishing a Global Connection Network with the option of encryption
Agenda

1. The IT Service Provider Finanz Informatik
2. Initial situation and objectives
3. Overview of changes
4. TCP/IP customizations
5. VTAM customizations
6. Paths in the APPN network
7. Customization for data encryption
8. The result
9. Gained experiences
10. Troubleshooting and solved problems
Overview of changes

**VTAM**
- Change the routing in the APPN Network
  - IBMTGEP
  - APPNCOS
  - Switch Major Nodes for BN-BN Connections
  - XCA Major Node

**TCP/IP**
- IP address concept for the GCN
- New static VIPAs
- OSPF
- Policy Agent
- IKED
Agenda

1. The IT Service Provider Finanz Informatik
2. Initial situation and objectives
3. Overview of changes
4. TCP/IP customizations
5. VTAM customizations
6. Paths in the APPN network
7. Customization for data encryption
8. The result
9. Gained experiences
10. Troubleshooting and solved problems
TCP/IP customizations (1/3)

Global Connection Network
- Additional static VIPAs are used exclusively for the Global Connection Network
- New OSPF interface for the additional VIPAs (ADVERTISE_VIPA_ROUTES=HOST_ONLY)

Encryption
- IPSec definition in the Policy Agent
- Internet Key Exchange Daemon (iked)
- Certificate
Sample

- Each location needs a separate Class C network for the Global Connection Network.
- Distribution of the individual IP addresses on each host.
TCP/IP customizations

**ADVERTISE_VIPA_ROUTES=Host_ONLY:**
- DESTINATION: **0.0.0.0**
- MASK: **0.0.0.0**
- ROUTE TYPE: SPIA
- DISTANCE: **31**
- AGE: **34172**
- NEXT HOP(S): 1.1.2.1 (Router1)
  1.1.3.1 (Router2)

**ADVERTISE_VIPA_ROUTES=Host_And_Subnet:**
- DESTINATION: **1.1.1.10**
- MASK: **255.255.255.0**
- ROUTE TYPE: SPF
- DISTANCE: **31**
- AGE: **34243**
- NEXT HOP(S): 1.1.2.11 (Router1)
  1.1.2.12 (Router1)
  1.1.2.13 (Router1)
  1.1.2.14 (Router1)
  ...
  1.1.3.11 (Router2)
  1.1.3.12 (Router2)
  1.1.3.13 (Router2)
  1.1.3.14 (Router2)

**ADVERTISE_VIPA_ROUTES=Host_And_Subnet (default):**
- Loss of OSPF on LPAR X
- From time to time APPN UDP packets reach the LPAR X via LPAR Z
- Result: No path switch in the APPN network

**Recommendation:** **ADVERTISE_VIPA_ROUTES=HOST_ONLY**...
Agenda

1. The IT Service Provider Finanz Informatik
2. Initial situation and objectives
3. Overview of changes
4. TCP/IP customizations
5. VTAM customizations
6. Paths in the APPN network
7. Customization for data encryption
8. The result
9. Gained experiences
10. Troubleshooting and solved problems
VTAM customizations

Extensions
• Enterprise Extender XCA Major Node (VNTYPE=GLOBAL)
• MODELRTXP (DYNTYPE=VN: DISCNT=NO)

Design change of routing
• Creating your own APPNCOS
• Adjustments of EE connections
  - between the BN of the different NetIDs
  - between the different nodes within a NetID
## VTAM customizations

### VTAM Customizations

<table>
<thead>
<tr>
<th></th>
<th>EN (NetID A / NetID B)</th>
<th>BN (NetID A / NetID B)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>WEIGHT</td>
<td>WEIGHT</td>
</tr>
<tr>
<td>XCF (native APPN)</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td>EE (NetID A)</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>GCN (BN)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>GCN (EN)</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

### #CONNECT

<table>
<thead>
<tr>
<th></th>
<th>EN (NetID A / NetID B)</th>
<th>BN (NetID A / NetID B)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>WEIGHT</td>
<td>WEIGHT</td>
</tr>
<tr>
<td>XCF (native APPN)</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>EE (NetID A)</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td>GCN (BN)</td>
<td>105</td>
<td>120</td>
</tr>
<tr>
<td>GCN (EN)</td>
<td>90</td>
<td>105</td>
</tr>
</tbody>
</table>

---

**Inside a NetID / Cross NetID**
VTAM customizations (3/5)

XCA Major Node definitions for the Global Connection Network:

...  

XCA G C N  GROUP D I A L = Y E S ,  
AUT O G E N = ( 2 5 0 , L X G C N , P X G C N . ) ,  
L I V T I M E = ( 5 , 0 ) , S R Q T I M E = 3 , S R Q R E T R Y = 3 ,  
I P A D D R = 1 . 1 . 1 . 1 ,  
V N N A M E = N E T I D A . C P N A M E A ,  
V N T Y P E = G L O B A L ,  
T G P = T G P G C N ,  
E E V E R I F Y = N E V E R ,  
A N S W E R = O N ,  
C A L L = I N O U T ,  
I S T A T U S = A C T I V E
Sample of IBMTGPS

XCF TGP COSTTIME=0,COSTBYTE=0,SECURITY=SECURE,
PDELAY=NEGLIGIB,CAPACITY=100M

* LAN Connections

LAN TGP COSTTIME=0,COSTBYTE=64,SECURITY=UNSECURE,
PDELAY=TERRESTR,CAPACITY=1G

* WAN Connections for GCN

TGPGCN TGP COSTTIME=0,COSTBYTE=0,SECURITY=SECURE,
PDELAY=TERRESTR,CAPACITY=1G
VTAM customizations

Sample of APPNCOS

CPSVCMG APPNCOS PRIORITY=NETWORK,NUMBER=8 transmission priority
   LINEROW WEIGHT=30, line row weight *
   NUMBER=1, line row number *
   ....
   CAPACITY=(100M,100M), line speed *
   COSTTIME=(0,0), cost per connect time *
   COSTBYTE=(0,0), cost per byte transmitted *
   PDELAY=(MINIMUM,NEGLIGIB), propagation delay *
   SECURITY=(SECURE,MAXIMUM) security level for TG
...

#CONNECT APPNCOS PRIORITY=MEDIUM,NUMBER=8 transmission priority A1R ...

   LINEROW WEIGHT=90, line row weight *
   NUMBER=3, line row number *
   ....
   CAPACITY=(1G,MAXIMUM), line speed *
   COSTTIME=(0,0), cost per connect time *
   COSTBYTE=(0,0), cost per byte transmitted *
   PDELAY=(MINIMUM,TERRESTR), propagation delay *
   SECURITY=(SECURE,MAXIMUM) security level for TG
Agenda

1. The IT Service Provider Finanz Informatik
2. Initial situation and objectives
3. Overview of changes
4. TCP/IP customizations
5. VTAM customizations
6. Paths in the APPN network
7. Customization for data encryption
8. The result
9. Gained experiences
10. Troubleshooting and solved problems
Paths in the APPN network

- APPN/EE
- Weight 150
- Global Connection Network
- Weight 90 - 120
- Weight 150
- Weight 30/60
- Weight 60/30

Diagram showing network paths and weights.
Agenda

1. The IT Service Provider Finanz Informatik
2. Initial situation and objectives
3. Overview of changes
4. TCP/IP customizations
5. VTAM customizations
6. Paths in the APPN network
7. Customization for data encryption
8. The result
9. Gained experiences
10. Troubleshooting and solved problems
Customization for data encryption (1/2)

Components

- IKED Daemon incl. certificate (each Host)
- Policy Agent
- Traffic Regulation Manager Daemon
- IBM Configuration Assistant for z/OS
Customization for data encryption

IBM Configuration Assistant:

IPSec Perspective

TCP/IP stack information:

Enter the name of the TCP/IP stack: * TCPIP

Enter a description:

Click the Add... button for each connectivity rule you want to add to this stack.

<table>
<thead>
<tr>
<th>Local/Source</th>
<th>Remote/Destination</th>
<th>Requirement Map</th>
<th>Topology</th>
<th>Status</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.0/24</td>
<td>2.2.2.0/24</td>
<td>EE_IPSec</td>
<td>Host to Host</td>
<td>Enabled</td>
<td>A-B</td>
</tr>
<tr>
<td>1.1.1.0/24</td>
<td>3.3.3.0/24</td>
<td>EE_IPSec</td>
<td>Host to Host</td>
<td>Enabled</td>
<td>A-C</td>
</tr>
<tr>
<td>All_IPv4_Addresses</td>
<td>All_IPv4_Addresses</td>
<td>ALL_TRAFFIC</td>
<td>Filtering - Either</td>
<td>Enabled</td>
<td>PERMIT_ALL</td>
</tr>
</tbody>
</table>

Add...  Copy...  Modify Basics...  Delete  View Details...  Move Up  Health Check...

Modify Wizard...  

Main Perspective  Apply Changes  OK  Cancel  Help
Agenda

1. The IT Service Provider Finanz Informatik
2. Initial situation and objectives
3. Overview of changes
4. TCP/IP customizations
5. VTAM customizations
6. Paths in the APPN network
7. Customization for data encryption
8. The result
9. Gained experiences
10. Troubleshooting and solved problems
The result

1.1.1.0/24

1.1.1.0/24

2.2.2.0/24

2.2.2.0/24

APPN/EE

IPSec encryption

Global Connection Network

Weight 150

Weight 90 - 120
Agenda

1. The IT Service Provider Finanz Informatik
2. Initial situation and objectives
3. Overview of changes
4. TCP/IP customizations
5. VTAM customizations
6. Paths in the APPN network
7. Customization for data encryption
8. The result
9. Gained experiences
10. Troubleshooting and solved problems
Gained experiences

1. The Global Connection Network can also be used for data transmission between nodes of the same NetID.

2. APPN traffic can be seen at the udp ports 12000 – 12004. APPN encrypted traffic uses the IPsec protocol to transfer data. A reference to the ports 12000 – 12004 is not available.

3. QOS Definitions for APPN traffic do not apply to IPSec, if done based on portocol and port number (ip tos bits still get propagated into the network).

4. A CP-CP session along a Global Connection Network can not be established (you need direct EE-Connections!).

5. EE verification disabled for ipsec due to timing problems.
Agenda

1. The IT Service Provider Finanz Informatik
2. Initial situation and objectives
3. Overview of changes
4. TCP/IP customizations
5. VTAM customizations
6. Paths in the APPN network
7. Customization for data encryption
8. The result
9. Gained experiences
10. Troubleshooting and solved problems
Troubleshooting

SYSLOG: Dec 7 11:15:57 HOSTA TRMD.TCPIP 65561: EZD0818I Tunnel added: 12/07/2012 10:15:49.75 vpnaction= IPSec_Dyn_ESP tunnelID= Y1234 AHSPI= 0 ESPSPI= 1274239020

Open Edition Command: ipsec -p stackname -y display -a Y1234

<table>
<thead>
<tr>
<th>HOSTA</th>
<th>HOSTB</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS V1R12 ipsec Stack Name: TCPIP Fri Dec 7 11:33:40 2012</td>
<td>CS V1R12 ipsec Stack Name: TCPIP Fri Dec 7 11:39:40 2012</td>
</tr>
<tr>
<td>Primary: Dynamic tunnel Function: Display</td>
<td>Primary: Dynamic tunnel Function: Display</td>
</tr>
<tr>
<td>Format: Detail Source: Stack Scope: Current</td>
<td>Format: Detail Source: Stack Scope: Current</td>
</tr>
<tr>
<td>TotAvail: 157</td>
<td>TotAvail: 208</td>
</tr>
<tr>
<td>TunnelID: Y1234</td>
<td>TunnelID: Y5678</td>
</tr>
<tr>
<td>Generation: 4</td>
<td>Generation: 4</td>
</tr>
<tr>
<td>IKEVersion: 1.0</td>
<td>IKEVersion: 1.0</td>
</tr>
<tr>
<td>ParentIKETunnelID: K5</td>
<td>ParentIKETunnelID: K4299</td>
</tr>
<tr>
<td>VpnActionName: IPSec_Dyn_ESP</td>
<td>VpnActionName: IPSec_DYN_ESP</td>
</tr>
<tr>
<td>LocalDynVpnRule: n/a</td>
<td>LocalDynVpnRule: n/a</td>
</tr>
<tr>
<td>State: Active</td>
<td>State: Active</td>
</tr>
<tr>
<td>HowToEncap: Transport</td>
<td>HowToEncap: Transport</td>
</tr>
<tr>
<td>LocalEndPoint: 1.1.1.1</td>
<td>LocalEndPoint: 2.2.2.2</td>
</tr>
<tr>
<td>RemoteEndPoint: 2.2.2.2</td>
<td>RemoteEndPoint: 1.1.1.1</td>
</tr>
<tr>
<td>HowToAuth: ESP</td>
<td>HowToAuth: ESP</td>
</tr>
<tr>
<td>AuthAlgorithm: HMAC-SHA1</td>
<td>AuthAlgorithm: HMAC-SHA1</td>
</tr>
<tr>
<td>AuthInboundSpi: 1274239020 (0x4BF3582C)</td>
<td>AuthInboundSpi: 4215159708 (0xFB3E3B9C)</td>
</tr>
<tr>
<td>AuthOutboundSpi: 4215159708 (0xFB3E3B9C)</td>
<td>AuthOutboundSpi: 1274239020 (0x4BF3582C)</td>
</tr>
<tr>
<td>HowToEncrypt: AES-CBC</td>
<td>HowToEncrypt: AES-CBC</td>
</tr>
<tr>
<td>KeyLength: 128</td>
<td>KeyLength: 128</td>
</tr>
<tr>
<td>EncryptInboundSpi: 1274239020 (0x4BF3582C)</td>
<td>EncryptInboundSpi: 4215159708 (0xFB3E3B9C)</td>
</tr>
<tr>
<td>EncryptOutboundSpi: 4215159708 (0xFB3E3B9C)</td>
<td>EncryptOutboundSpi: 1274239020 (0x4BF3582C)</td>
</tr>
<tr>
<td>LocalPort: 12001</td>
<td>LocalPort: 12001</td>
</tr>
<tr>
<td>LocalPortRange: n/a</td>
<td>LocalPortRange: n/a</td>
</tr>
<tr>
<td>RemotePort: 12001</td>
<td>RemotePort: 12001</td>
</tr>
</tbody>
</table>
Solved problems

1. Hanging IPSec tunnel after IPL or restart IKED
   Solution: APAR PM62089

2. IKED abend S106
   Solution: APAR PM58292

3. EE connections cannot be established via a Global Connection Network after IPL or VTAM restart
   (Sense-Code 08060027 and 08090000)
   Solution: APAR OA39303
Questions?
Thank you for your attention.