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

Share Conference

Heinz Klümper (FI) & Matthias Burkhard (IBM)

February 03 - 08, 2013, San Francisco

Sparkassen-Finanzgruppe

finanz **informatik**

Personal Introduction

Heinz Klümper
(Finanz Informatik)

phone: +49 (0) 251 288-33697

email: heinz.kluemper@f-i.de

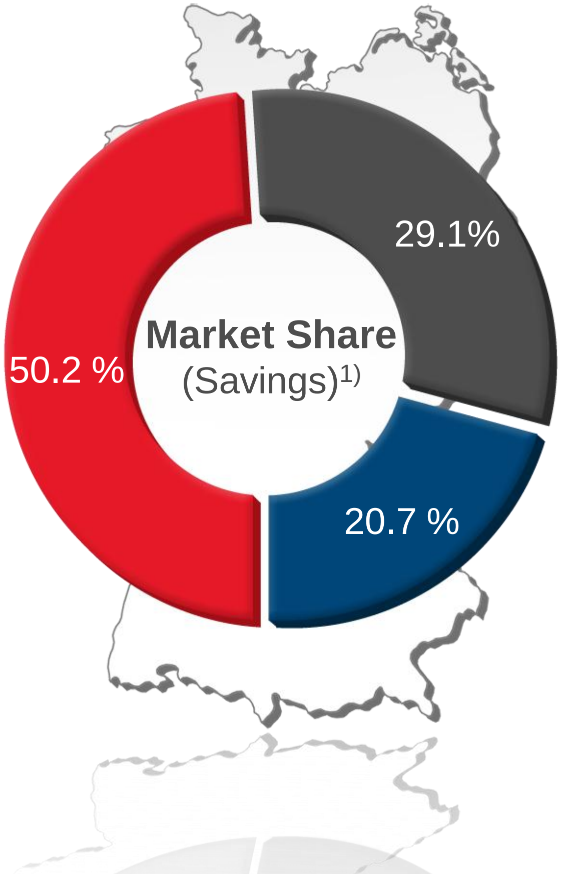
Agenda

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	
Revenue (in mill. €) (2011)	1,453
with saving banks	1,004
with state banks	229
Employees (full-time equivalents)	4,975

Customers	
Savings banks	423
State banks + DekaBank	9
State home loan banks	10
Accumulated balance sheet of supported savings banks (in bill. €) (2011)	1,046



🟥 Savings Banks Financial Group ⬛ Credit Unions 🟦 Private Banks, other

June 30th, 2012

[1] Sources: DSGV (12/31/2011); German Federal Bank, Others.

Significant scale can be achieved through bundling volume IT services

Supported financial institutions	
Branches of supported savings banks	15,250
Bank-specific employees of supported savings banks (2010)	192,301

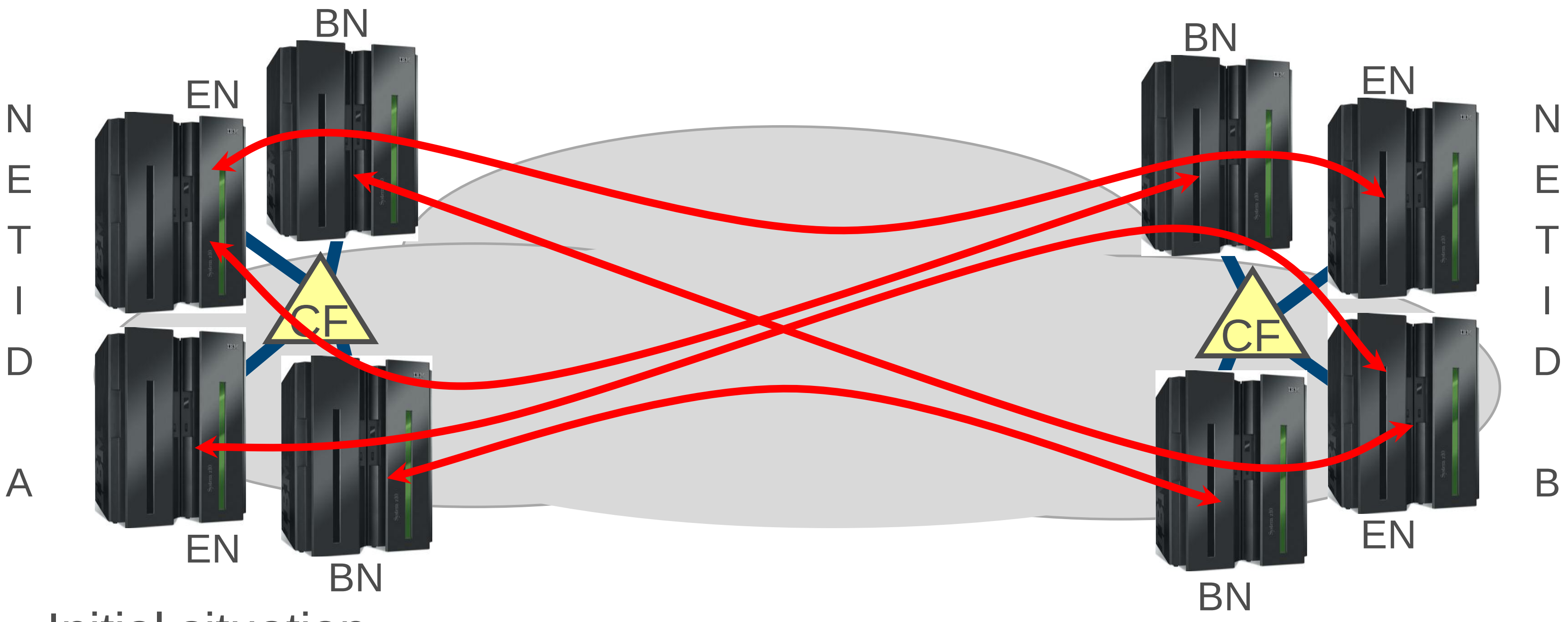
Processing volumes	
Booked entries per annum (in bill.)	11
Supported accounts (in mill.)	127

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 and objectives (1/2)



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
  - IBMTGPS
  - 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)

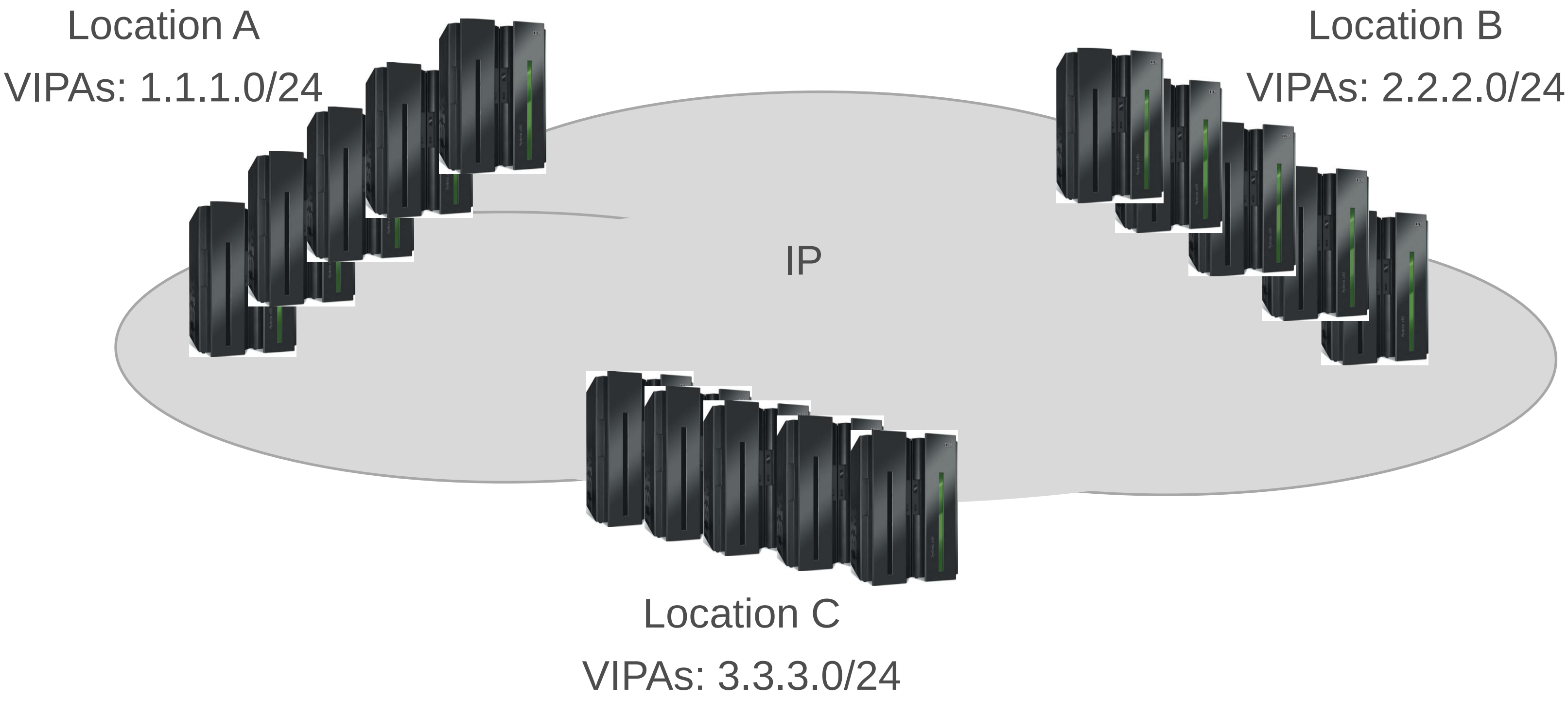
Global Connection Network

- 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

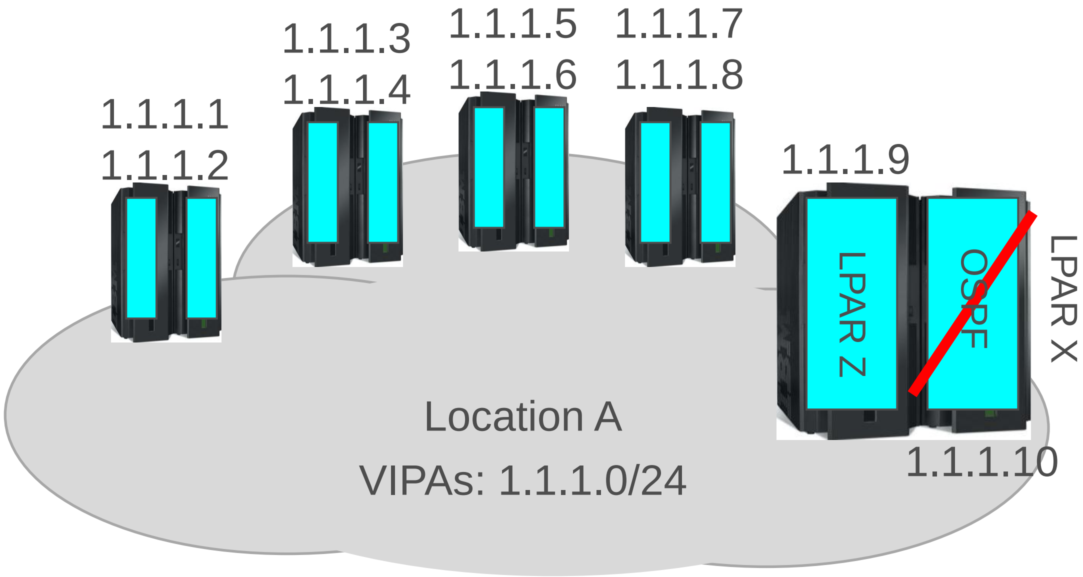
TCP/IP customizations (2/3)



Sample

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

TCP/IP customizations (3/3)



```
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 (1/5)

Extensions

- Enterprise Extender XCA Major Node (VNTYPE=GLOBAL)
- MODELRTP (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 (2/5)

CPSVCMG	EN (NetID A / NetID B) WEIGHT		BN (NetID A / NetID B) WEIGHT	
XCF (native APPN)	30	-	30	-
EE (NetID A)	60	-	60	150
GCN (BN)	-	-	-	-
GCN (EN)	-	-	-	-

#CONNECT	EN (NetID A / NetID B) WEIGHT		BN (NetID A / NetID B) WEIGHT	
XCF (native APPN)	60	-	60	-
EE (NetID A)	30	-	30	150
GCN (BN)	105	105	120	120
GCN (EN)	90	90	105	105

Inside a NetID / Cross NetID

VTAM customizations (3/5)

XCA Major Node definitions for the Global Connection Network:

```
...
XCAGCN         GROUP DIAL=YES,                                         *
               AUTOGEN=(250,LXXGCN,PXXGCN.),                           *
               LIVTIME=(5,0),SRQTIME=3,SRQRETRY=3,                     *
               IPADDR=1.1.1.1,          <- local IP-Addresse GCN       *
               VNNAME=NETIDA.CPNAMEA,   <- NetID & CPNAME GCN          *
               VNTYPE=GLOBAL,                                          *
               TGP=TGPGCN,              <- TGP from IBMTGPS            *
               EEVERIFY=NEVER,                                         *
               ANSWER=ON,                                              *
               CALL=INOUT,                                             *
               ISTATUS=ACTIVE
```

VTAM customizations (4/5)

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 (5/5)

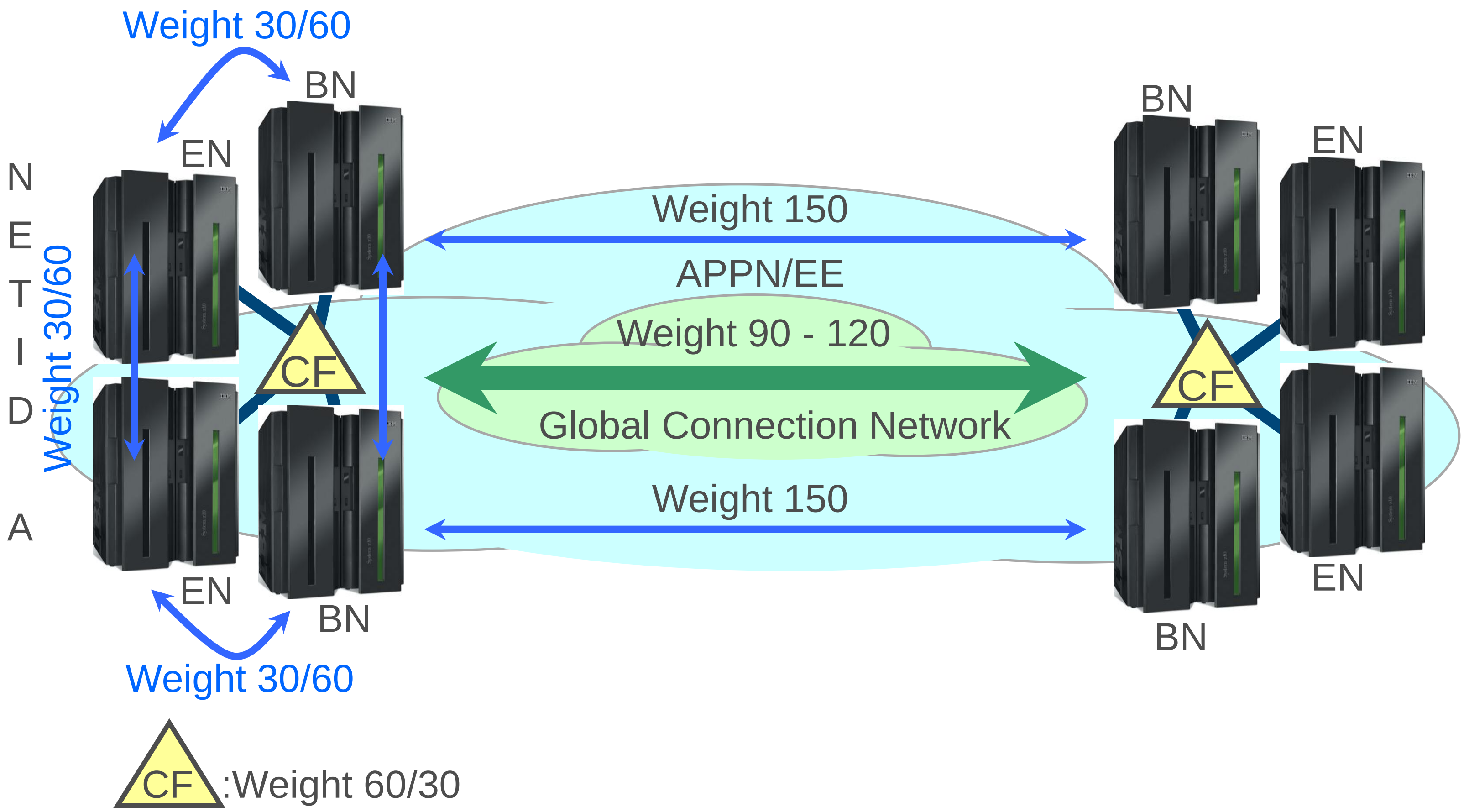
Sample of APPNCOS

```
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

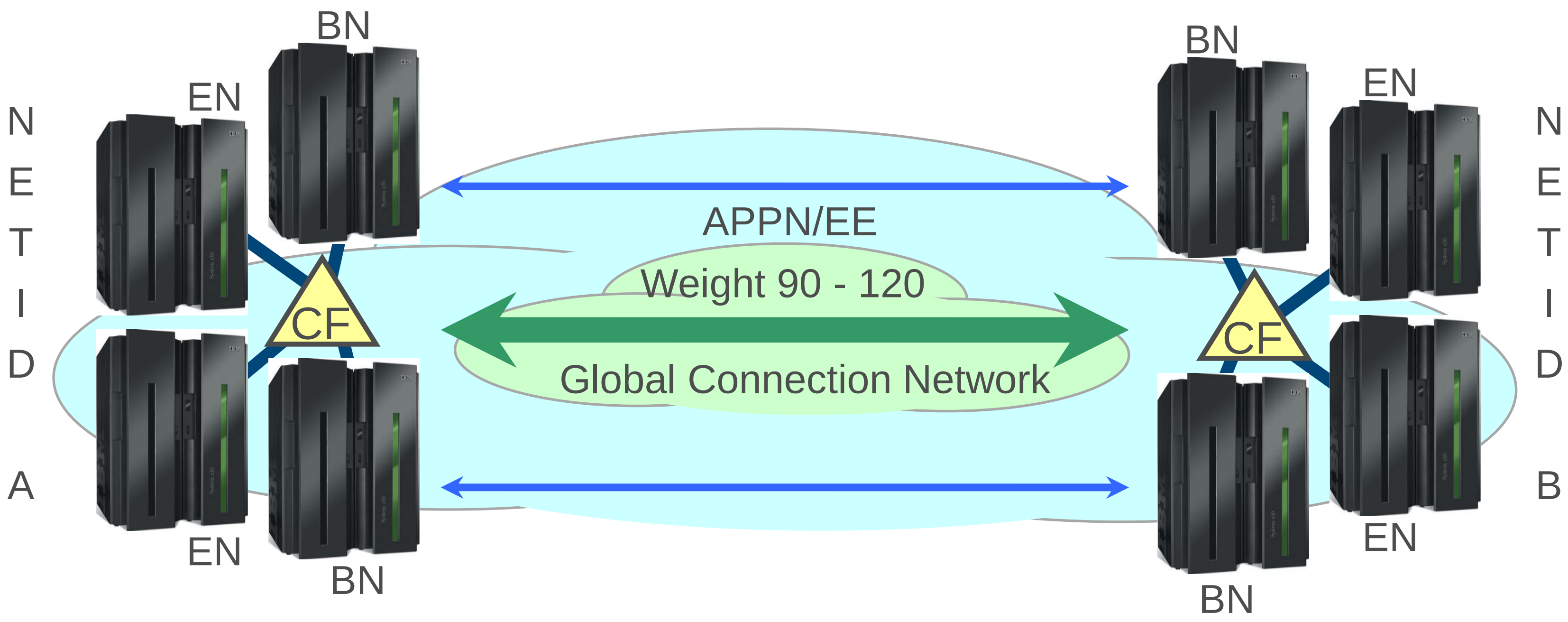
Paths in the APPN network



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)

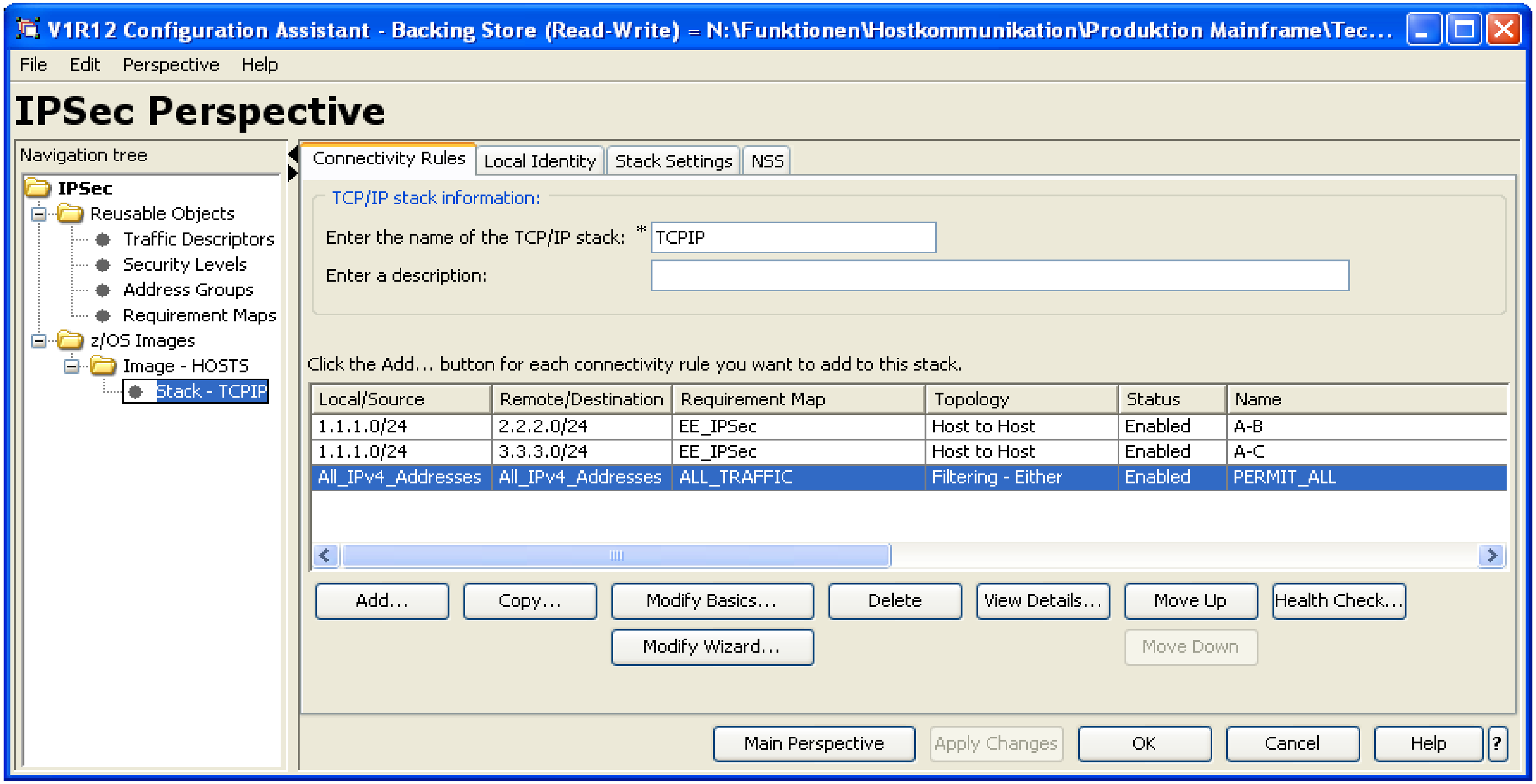


Components

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

Customization for data encryption (2/2)

IBM Configuration Assistant:



V1R12 Configuration Assistant - Backing Store (Read-Write) = N:\Funktionen\Hostkommunikation\Produktion Mainframe\Tec...

IPSec Perspective

TCP/IP stack information:

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

Enter a description:

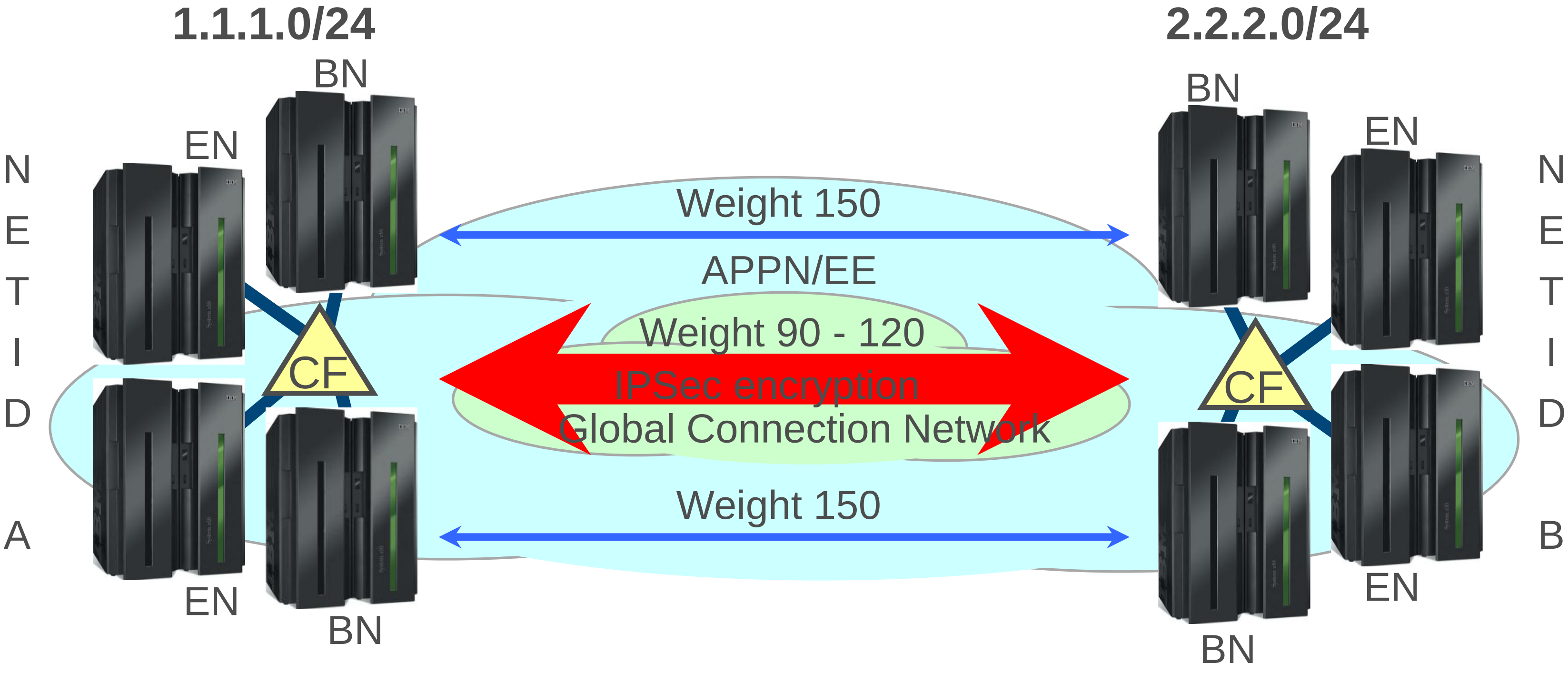
Click the Add... button for each connectivity rule you want to add to this stack.

Local/Source	Remote/Destination	Requirement Map	Topology	Status	Name
1.1.1.0/24	2.2.2.0/24	EE_IPSec	Host to Host	Enabled	A-B
1.1.1.0/24	3.3.3.0/24	EE_IPSec	Host to Host	Enabled	A-C
All_IPv4_Addresses	All_IPv4_Addresses	ALL_TRAFFIC	Filtering - Either	Enabled	PERMIT_ALL

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
2.2.2.0/24
N E T I D A
N E T I D B
BN
EN
EN
BN
CF
BN
EN
EN
BN
CF
Weight 150
APPN/EE
Weight 90 - 120
IPSec encryption
Global Connection Network
Weight 150

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

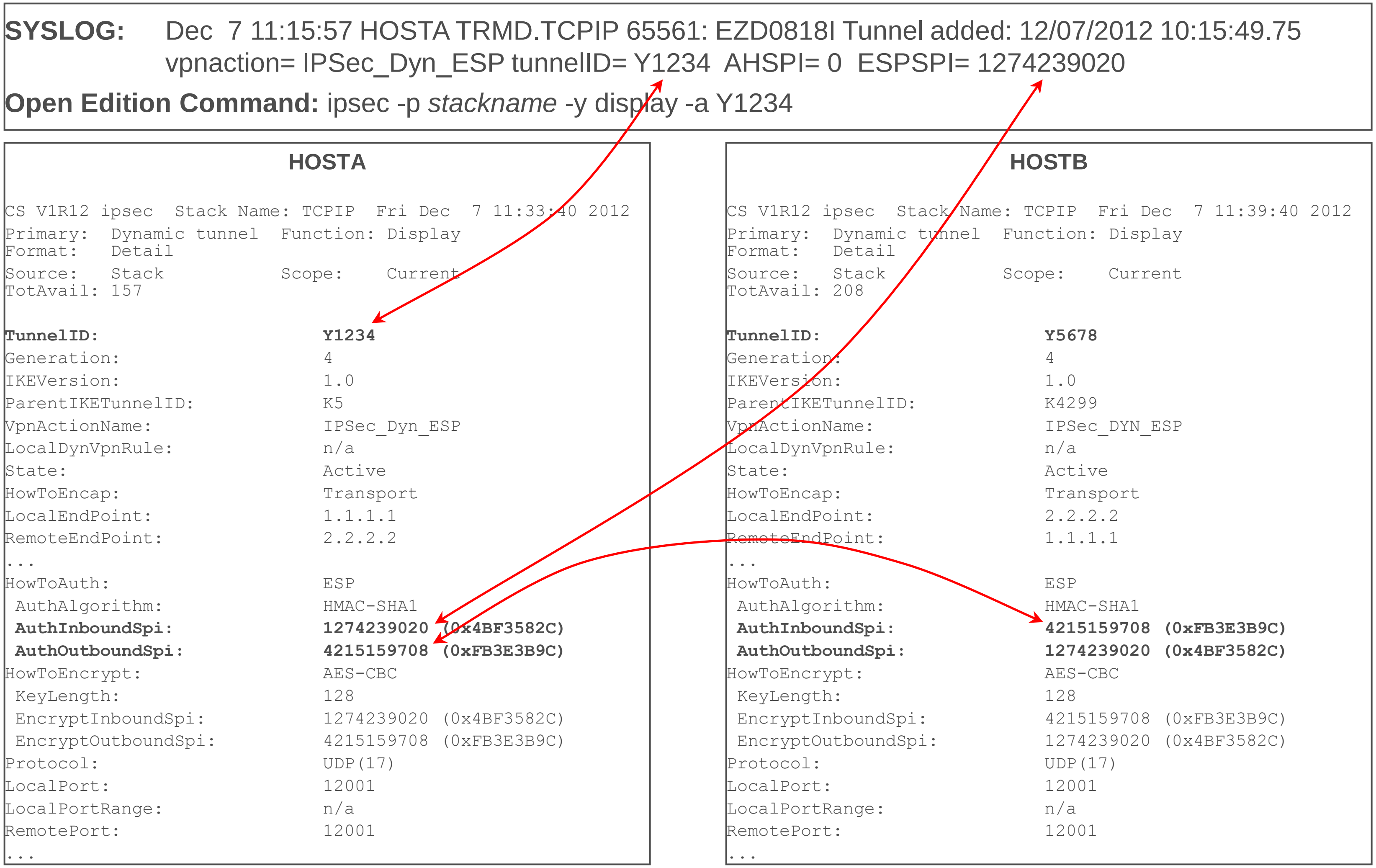
Gained experiences

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

HOSTA

```
CS V1R12 ipsec  Stack Name: TCPIP  Fri Dec  7 11:33:40 2012
Primary:  Dynamic tunnel  Function: Display
Format:   Detail
Source:   Stack           Scope:    Current
TotAvail: 157

TunnelID:                     Y1234
Generation:                   4
IKEVersion:                   1.0
ParentIKETunnelID:            K5
VpnActionName:                IPSec_Dyn_ESP
LocalDynVpnRule:              n/a
State:                        Active
HowToEncap:                   Transport
LocalEndPoint:                1.1.1.1
RemoteEndPoint:               2.2.2.2
...
HowToAuth:                    ESP
 AuthAlgorithm:               HMAC-SHA1
 AuthInboundSpi:              1274239020 (0x4BF3582C)
 AuthOutboundSpi:             4215159708 (0xFB3E3B9C)
HowToEncrypt:                 AES-CBC
 KeyLength:                   128
 EncryptInboundSpi:           1274239020 (0x4BF3582C)
 EncryptOutboundSpi:          4215159708 (0xFB3E3B9C)
Protocol:                     UDP(17)
LocalPort:                    12001
LocalPortRange:               n/a
RemotePort:                   12001
...
```

HOSTB

```
CS V1R12 ipsec  Stack Name: TCPIP  Fri Dec  7 11:39:40 2012
Primary:  Dynamic tunnel  Function: Display
Format:   Detail
Source:   Stack           Scope:    Current
TotAvail: 208

TunnelID:                     Y5678
Generation:                   4
IKEVersion:                   1.0
ParentIKETunnelID:            K4299
VpnActionName:                IPSec_DYN_ESP
LocalDynVpnRule:              n/a
State:                        Active
HowToEncap:                   Transport
LocalEndPoint:                2.2.2.2
RemoteEndPoint:               1.1.1.1
...
HowToAuth:                    ESP
 AuthAlgorithm:               HMAC-SHA1
 AuthInboundSpi:              4215159708 (0xFB3E3B9C)
 AuthOutboundSpi:             1274239020 (0x4BF3582C)
HowToEncrypt:                 AES-CBC
 KeyLength:                   128
 EncryptInboundSpi:           4215159708 (0xFB3E3B9C)
 EncryptOutboundSpi:          1274239020 (0x4BF3582C)
Protocol:                     UDP(17)
LocalPort:                    12001
LocalPortRange:               n/a
RemotePort:                   12001
...
```

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.