iSeries

Configurar ligações da Central de Gestão para ambientes de firewall

Relatório da Experiência

iSeries

Configurar ligações da Central de Gestão para ambientes de firewall

Índice

Configurar ligações da Central de Gestão para ambientes de firewall

Este relatório explica em detalhe as ligações da Central de Gestão e as configurações necessárias para activar a Central de Gestão para funcionar numa variedade de ambientes de firewall a partir da v5r3. Tal como uma aplicação de gestão distribuída, a Central de Gestão requer numerosas ligações de entrada e de saída do terminal TCP/IP. Pelo contrário, a premissa básica de uma firewall é restringir/modificar ligações de entrada e de saída. Para ajudar na configuração da Central de Gestão num ambiente de firewall, este relatório aborda a natureza e orientação das ligações da Central de Gestão, bem como as restrições de tipos específicos de firewalls que limitam ou desactivam algumas ligações da Central de Gestão. A Tradução do endereço de rede estática (NAT - Network Address Translation) e a Tradução do endereço de rede dinâmica serão abordadas. Serão descritos três ambientes de firewall básicos juntamente com a configuração necessária para activar a Central de Gestão de modo a que funcione adequadamente em cada ambiente. Estes ambientes básicos e configurações associadas destinam-se a ser utilizados como guias para a activação da Central de Gestão em ambientes de firewall mais complexos.

Terminologia
Define termos importantes que serão utilizados ao longo deste relatório.

Ligações da Central de Gestão
Descreve as diferentes ligações estabelecidas entre o Cliente Gráfico e os servidores da Central de Gestão. Agrupa as aplicações pelas que utilizam cada uma das ligações.

Referência rápida da firewall da Central de Gestão
Um gráfico que lista as portas que é necessário abrir nas firewalls, de modo a que a Central de Gestão funcione num caso simples (não é válido se a tradução do endereço de rede estiver a ser utilizada).

Limitações da Central de Gestão devido à Tradução do endereço de rede
Descreve a tradução do endereço de rede estática e dinâmica e o modo como estes tipos de tradução do endereço afectam a Central de Gestão.

Cenário 1 - Cliente Gráfico protegido por uma firewall
Apresenta em detalhe a configuração necessária para activar a Central de Gestão quando o Cliente Gráfico está protegido do resto da rede por uma firewall.

Cenário 2 - Sistema Central protegido por uma firewall
Apresenta em detalhe a configuração necessária para activar a Central de Gestão quando os servidores do Sistema Central e do Sistema de Destino Final estão protegidos de Clientes Gráficos e do resto da rede por uma firewall comum.

Cenário 3 - Sistemas de Destino Final protegidos por uma firewall
Apresenta em detalhe a configuração necessária para activar a Central de Gestão quando os servidores do Sistema de Destino Final estão protegidos do Sistema Central, do Sistema Origem e do resto da rede por uma firewall comum.

Capítulo 1. Terminologia

É importante definir claramente alguns termos chave. Alguns termos associados à Central de Gestão e firewalls são ambíguos, de modo que é importante a definição clara dos mesmos no início. Os termos que são utilizados neste documento referem-se exactamente ao que é especificado na definição (a menos que seja indicado o contrário).

Sistema Central (CS)
Sistema iSeries(TM) que é utilizado para gerir outros sistemas iSeries. O Sistema Central (CS - Central System) da Central de Gestão (MC - Management Central) envia pedidos e recebe respostas dos Sistemas de Destino Final da Central de Gestão para executar tarefas e serviços de supervisão. Os dados da Central de Gestão, incluindo o sistema, inventário, tarefa e supervisão, estão armazenados no iSeries do Sistema Central. Cada sistema iSeries está activado para gerir como um Sistema Central da Central de Gestão e para ser gerido como um Sistema de Destino Final da Central de Gestão.

Tradução do endereço da rede dinâmica (NAT dinâmico)
Mapeamento de um endereço de IP local para o primeiro endereço de IP disponível numa área de endereços de IP globais. A maioria das firewalls têm esta opção e permite-lhe especificar NAT dinâmico, NAT estático ou não utilizar o NAT numa ligação. Também pode ser conhecido como Tradução do endereço da porta (PAT - Port Address Translation), NAT de endereço único, NAT com canais múltiplos ao nível da porta e Sobrecarga. Todos estes tópicos serão referenciados neste documento como NAT dinâmico.

Sistema de Destino Final (EP)
Sistema iSeries que é gerido por um Sistema Central iSeries. O Sistema Central da MC envia pedidos e recebe respostas dos Sistemas de Destino Final da Central de Gestão para executar tarefas e serviços de supervisão. Cada sistema iSeries está activado para gerir como um Sistema Central da Central de gestão e para ser gerido como um Sistema de Destino Final da Central de Gestão.

Servidor do sistema central iSeries
Servidor que é executado no iSeries e que recebe e processa pedidos a partir de clientes do iSeries Navigator. Estes servidores do sistema central têm objectivos diferentes e fornecem grande parte da funcionalidade do sistema único do iSeries Navigator (isto inclui a maioria das funções localizadas para um sistema no contentor My Connections [As minhas ligações]).

Central de Gestão (MC)
A Central de Gestão (MC - Management Central) é uma arquitectura distribuída de três escalões que hospeda um conjunto de aplicações de Gestão de sistemas iSeries. A Central de Gestão envolve as infra-estruturas de classe baseadas em C++ e em Java(TM) implementadas nos Clientes Gráficos do iSeries Navigator (Operations Navigator na V5R1) e servidores do Sistema Central e do Sistema de Destino Final da MC do iSeries.

Aplicação da Central de Gestão
Conjunto de funções relacionadas que utiliza a infra-estrutura da Central de Gestão. Por exemplo, a Supervisão do sistema é uma aplicação da Central de Gestão que fornece supervisão distribuída das métricas de desempenho ao nível do sistema iSeries com vistas de gráficos, limiares e primitivas de automatização. O Comando remoto é uma aplicação da Central de Gestão que fornece definições persistentes do comando iSeries, execução e rastreio do comando distribuído.

Infra-estrutura em C++ da Central de Gestão
Arquitectura distribuída da MC implementada como uma biblioteca de classes C++ que permite um conjunto amplo de blocos de criação de aplicações incluindo: comunicação, persistência, distribuição, processamento assíncrono e processamento síncrono. A infra-estrutura em C++ da

MC está disponível nos Clientes Gráficos do iSeries Navigator (Operations Navigator na V5R1) e servidores do Sistema Central e do Sistema de Destino Final da MC do iSeries.

Infra-estrutura em Java da Central de Gestão
Arquitectura distribuída da MC implementada como uma biblioteca de classes Java que permite um conjunto amplo de blocos de criação de aplicações incluindo: comunicação, persistência, distribuição, processamento assíncrono e processamento síncrono. A infra-estrutura em Java da MC está disponível nos Clientes Gráficos do iSeries Navigator (Operations Navigator na V5R1) e servidores do Sistema Central e do Sistema de Destino Final da MC do iSeries.

Sistema Origem (ou Sistema Modelo)
Sistema iSeries utilizado como uma origem ou modelo para os dados da aplicação da Central de Gestão. Por exemplo, a aplicação Distribuição de software selecciona um Sistema Origem a partir do qual todos os Sistemas de Destino deverão obter os itens de uma distribuição de pacotes. A aplicação Comparar e actualizar correcções selecciona o Sistema Modelo ao qual todos os Sistemas de Destino são comparados (e a partir do qual são possivelmente actualizados).

Tradução do endereço de rede estática (NAT estático)
Mapeamento de um endereço de IP interno para um endereço de IP externo específico (e inalterável). Mapeamento estático um-para-um. A maioria das firewalls têm esta opção e permite-lhe especificar NAT dinâmico, NAT estático ou não utilizar o NAT numa ligação.

Sistemas de Destino
Sistemas iSeries que são os destinos ou receptores de dados ou acções da aplicação da Central de Gestão. Por exemplo, o sistema ou sistemas utilizados como destino para a tarefa Compare and Update of Fixes (Comparação e actualização de correcções) (ou outra tarefa semelhante). Estes são os sistemas que são comparados ao Sistema Origem (ou Sistema Modelo) e actualizados, se for necessário.

Capítulo 2. Ligações da Central de Gestão

Figura 1. Descrição geral das ligações da Central de Gestão

A seguinte secção fornece uma descrição geral das ligações da Central de Gestão (MC - Management Central) relativamente à infra-estrutura, aplicações, terminais protegidos e configurações de ligação.

A Central de Gestão é uma arquitectura com três escalões que activa a gestão de vários sistemas a partir de Clientes Gráficos do iSeries(TM) Navigator (Operations Navigator na V5R1) através de um iSeries de Sistema Central (CS - Central System). A arquitectura da Central de Gestão é constituída por duas infra-estruturas distintas, mas semelhantes, e distribuídas: uma implementada em C++ e a outra implementada em Java(TM). No que diz respeito à V5R3, a infra-estrutura em C++ está a ser faseada e substituída pela infra-estrutura em Java. Nos clientes gráficos, as infra-estruturas em C++ e em Java interoperam nos processos do iSeries Navigator. Nos servidores iSeries, as infra-estruturas em C++ e em Java da Central de Gestão funcionam independentemente em dois trabalhos daemons distintos de longa execução: C++ em QYPSSRV e Java em QYPSJSVR. Relativamente à V5R3, existe apenas o trabalho QYPSJSVR e suporta as funções que o trabalho QYPSSRV suportava na V5R2 e anterior. As características e restrições das ligações TCP/IP estabelecidas pelas implementações das infra-estruturas em C++ e em Java da Central de Gestão são únicas. Deste modo, as aplicações da Central de Gestão activadas por cada uma das infra-estruturas estão sujeitas a essas características e restrições.

Nem sempre é fácil determinar as portas que são utilizadas para cada aplicação da MC em cada sistema, porque a Central de Gestão utiliza duas infra-estruturas e dois servidores na V5R2 e edições anteriores, e agora na V5R3 utiliza apenas o servidor Java. As seguintes secções descrevem detalhadamente as portas que são utilizadas para cada aplicação da MC, mas se o utilizador estiver a planear utilizar algumas aplicações da MC ou se pretender abrir todas as portas da MC, mesmo que um ou duas não sejam utilizadas, é possível efectuar uma leitura rápida desta secção. É possível tomar nota das portas que estão

a ser utilizadas e das outras propriedades que é necessário definir, e não se preocupar sobre quais as aplicações específicas que utilizam as portas ou as propriedades.

Infra-estrutura em C++

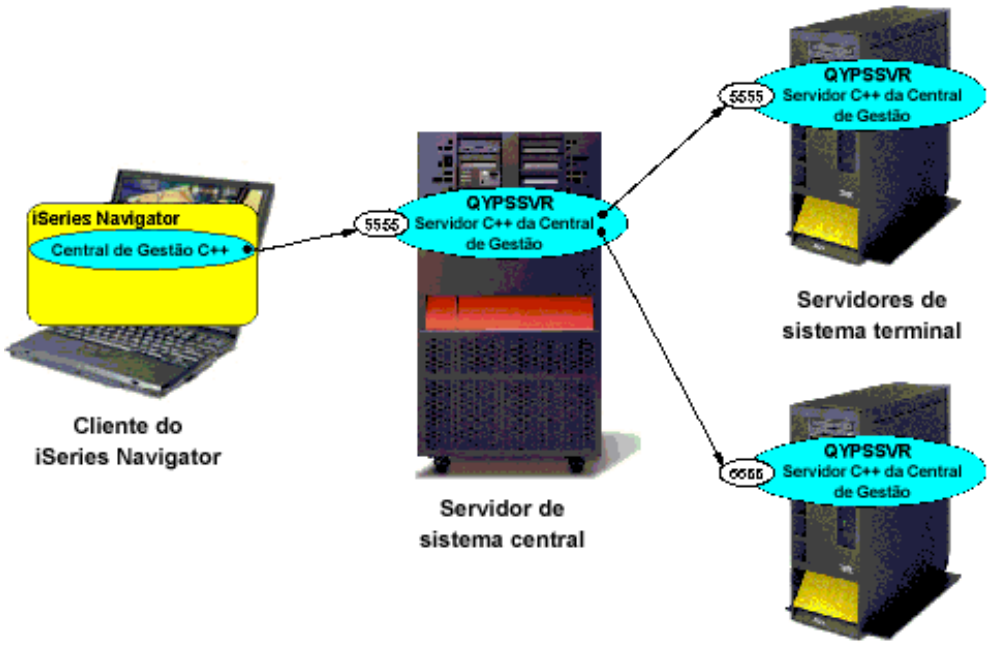

Figura 2. Ligações da infra-estrutura em C++ para a Central de Gestão

O diagrama acima representa as portas e ligações estabelecidas pela infra-estrutura em C++ introduzida na oferta inicial da Central de Gestão V4R3. A implementação da infra-estrutura em C++ cria um terminal TCP/IP de ponto a ponto a partir de cada Cliente Gráfico para o servidor (QYPSSRV) do Sistema Central, bem como a partir do servidor do Sistema Central para cada servidor (QYPSSRV) do Sistema de Destino Final. Os pacotes são recebidos e enviados bidireccionalmente na ligação única do terminal entre dois sistemas. O número da porta para ligações de entrada ao servidor C++ será assumido como 5555 e é configurável em cada servidor iSeries através das Entradas da tabela de assistência (Consulte a secção ″Configurações da ligação″). A infra-estrutura em C++ nem sempre tenta estabelecer uma ligação ao Cliente Gráfico a partir de um servidor iSeries.

Na V5R3, o servidor C++ (QYPSSRV) já não existe e o trabalho QYPSJSVR controla o trabalho que era executado pelo QYPSSRV. Deste modo, na V5R3 o QUAFFS receberá ligações de entrada na porta 5555 (bem como na porta 5544). Os servidores C++ com os sistemas v5r1 e V5R2 irão estabelecer ligação aos servidores Java (QYPSJSVR) nos sistemas V5R3 utilizando a porta 5555. O diagrama acima mostra um servidor C++ em cada iSeries, embora na V5R3 estes servidores sejam substituídos por QYPSJSVR que irá efectuar a recepção na porta 5555.

A partir da V5R2, a infra-estrutura em C++ da Central de Gestão activa as seguintes aplicações:

- Supervisores do sistema
- Histórico de gráficos
- Serviços de recolha
- Inventário
- Utilizadores e grupos (excepto Enviar utilizador)
- Executar comando
- Instalar produtos
- Correcções (excepto Enviar correcções)

Em sistemas V5R3, estas aplicações são executadas através da infra-estrutura em Java da Central de Gestão (que é descrita numa secção posterior). Deste modo, quando estas aplicações são executadas entre sistemas V5R3, comunicam utilizando a porta da infra-estrutura em Java e quando são executadas entre sistemas V5R2 (ou entre um sistema V5R2 e um sistema V5R3) utilizam a porta da infra-estrutura em CA++.

Extensões CA++

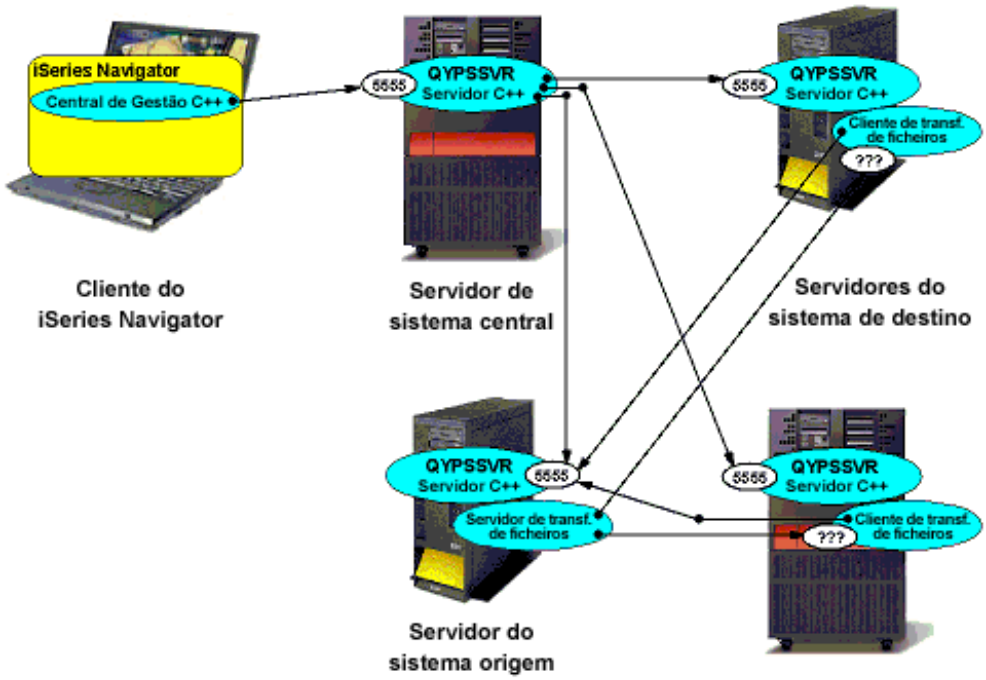

Figura 3. Ligações para extensões CA++ da Central de Gestão

A infra-estrutura em CA++ nos servidores iSeries oferece uma função de transferência de ficheiros [Transferência em massa de dados (BDT - Bulk Data Transfer)] entre um servidor origem e vários servidores de destino iSeries. A função de transferência de ficheiros está implementada como um trabalho de transferência do cliente em cada servidor de destino e um trabalho de transferência do servidor no servidor origem. O diagrama acima representa a extensão das portas da infra-estrutura em CA++ e as ligações às mesmas, bem como as ligações estabelecidas pela funcionalidade de transferência de ficheiros introduzida na oferta da Central de Gestão VA. Além das ligações do Cliente Gráfico ao servidor do

Sistema Central e do servidor do Sistema Central a cada servidor do Sistema de Destino Final, é estabelecida uma ligação do terminal TCP/IP ponto a ponto de ondas curtas a partir de um cliente de transferência de ficheiros em cada Sistema de Destino ao servidor do Sistema Origem (QUIPS). O cliente da transferência de ficheiros determina e comunica o respectivo endereço de IP de marcação após verificação do ID chamador e número da porta para o servidor de transferência de ficheiros nesta ligação de terminal de curta duração. O cliente da transferência de ficheiros determina o respectivo endereço de IP de marcação após verificação do ID chamador através das chamadas de getHostName e de getHostByName.

O nome do sistema central do Sistema de Destino é configurável em todos os servidores iSeries através da propriedade QYPS_HOSTNAME (Consulte a secção ″Configurações da ligação″). Subsequentemente, é estabelecida uma ligação de marcação após verificação do ID chamador do terminal TCP/IP a partir de um servidor de transferência de ficheiros associado no Sistema Origem ao cliente da transferência de ficheiros em cada Sistema de Destino. Tal como com a infra-estrutura em C++, o número da porta para ligações de entrada no servidor do Sistema Origem (QYPSSRV) será assumido como 5555. Como valor assumido, o número da porta da ligação de marcação após verificação do ID chamador da transferência de ficheiros será superior a 1024 e escolhido aleatoriamente no Sistema de Destino. Nos sistemas V5R2 e posterior, é possível configurar um intervalo de números de portas para a ligação de marcação após verificação do ID chamador da transferência de ficheiros em cada servidor através das propriedades de configuração da Central de Gestão (Consulte a secção ″Configurações da ligação″).

A partir da V5R2, as seguintes aplicações da Central de Gestão activadas pela infra-estrutura em V5R2++ optimizam também a funcionalidade de transferência de ficheiros C++:

- Distribuição de pacotes
- Enviar produtos
- Enviar utilizador
- Enviar correcções

Tal como mencionado na secção ″Infra-estrutura em C++″ acima, na V5R3 o servidor Java controla o servidor C++ e o trabalho QYPSSRV não existe. Deste modo, em sistemas V5R3 as aplicações acima mencionadas são executadas utilizando a infra-estrutura em Java e as extensões Java da Central de Gestão (que são descritas em secções posteriores). Isto significa que quando estas aplicações são executadas entre sistemas V5R3, comunicam utilizando as portas de extensão Java e infra-estrutura em Java, e quando estas aplicações são executadas entre sistemas V5R2 (ou entre um sistema V5R2 e um sistema V5R3), utilizam a infra-estrutura em C++ bem como as portas de extensão.

Infra-estrutura em Java

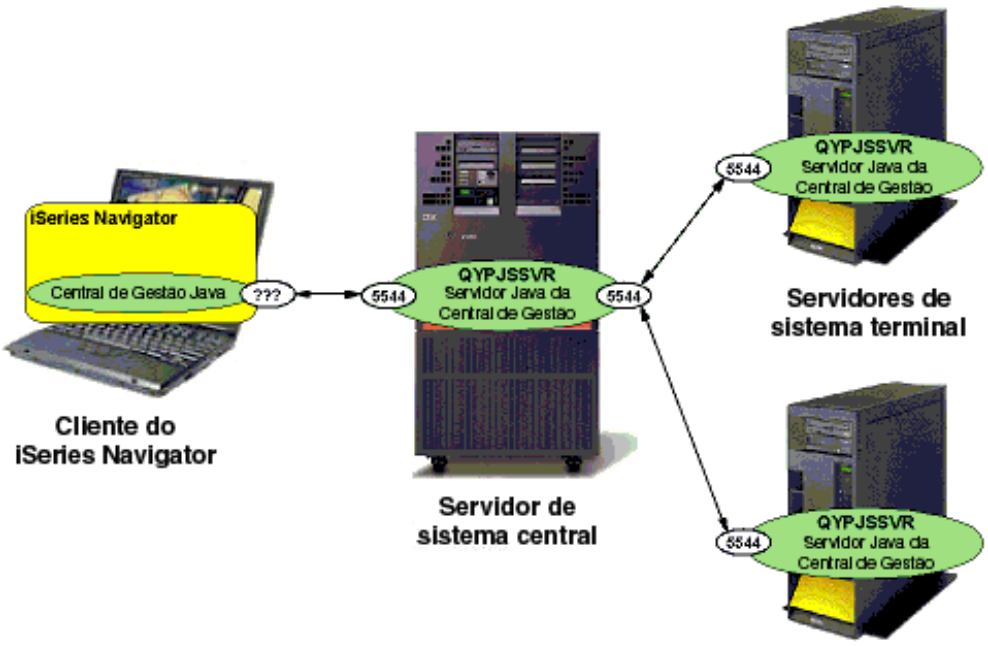

Figura 4. Ligações da infra-estrutura em Java para a Central de Gestão

O diagrama acima representa as portas e ligações estabelecidas pela infra-estrutura em Java introduzida na oferta da Central de Gestão V5R1. A infra-estrutura em Java optimiza a tecnologia Remote Method Invocation (RMI) de Java para estabelecer ligações entre Clientes Gráficos e servidores iSeries (QYPSJSVR). O RMI estabelece e mantém ligações de terminal TCP/IP e efectua o fluxo de dados ordenados de RMI entre sistemas. Um efeito secundário da funcionalidade RMI (Referências/objectos remotos) frequentemente optimizado pela infra-estrutura em Java, requer que os terminais TCP/IP sejam estabelecidos nas duas direcções entre cada sistema. O RMI produz dados ordenados para cada Referência remota que contém o número da porta e o nome do sistema central da marcação após verificação do ID chamador. Estes dados ordenados (incluindo o nome do sistema central e o número da porta) encontram-se no protocolo de RMI e não estão disponíveis para tradução dinâmica. Cada sistema determina o respectivo nome do sistema central através da chamada de getHostName. O nome do sistema central é configurável em cada Cliente Gráfico do iSeries Navigator e cada servidor iSeries através da propriedade QYPS_HOSTNAME (Consulte a secção ″Configurações da ligação″).

O nome do sistema central e o número da porta nos dados ordenados são utilizados por outros sistemas para contactar novamente com este sistema. O número da porta para ligações de entrada ao servidor Java (QYPSJSVR) será assumido como 5544 e é configurável em cada servidor iSeries através das Entradas da tabela de assistência (Consulte a secção ″Configurações da ligação″). O número da porta para ligações de entrada da infra-estrutura em Java ao Cliente Gráfico será escolhido como valor assumido aleatoriamente no sistema cliente e é configurável em cada sistema cliente através de um ficheiro de propriedades (Consulte a secção ″Configurações da ligação″). O nome do sistema central nos dados ordenados (que pode ser o nome do sistema central real ou um endereço de IP) representa o endereço que outros sistemas utilizarão para contactar com este sistema. Este nome do sistema central será assumido como o

endereço de IP que o sistema central reconhece como próprio e é configurável em cada Cliente Gráfico e servidor iSeries através da propriedade QYPS_HOSTNAME (Consulte a secção ″Configurações da ligação″).

A infra-estrutura em Java foi introduzida na oferta da Central de Gestão V5R1 e a partir da V5R3 activa as seguintes aplicações:

- Comparação e actualização dos valores do sistema
- Sincronizar data e hora
- Sincronizar funções
- Supervisor de trabalhos
- Supervisor de mensagens
- Supervisor de ficheiros
- Supervisores B2B
- Tarefas BRMS
- Agendar movimentos de recursos LPAR

As seguintes aplicações utilizam a infra-estrutura em Java em sistemas V5R3, mas utilizam a infra-estrutura em C++ em sistemas V5R2 e anteriores (consulte a secção ″Infra-estrutura em C++″ para obter detalhes):

- Supervisores do sistema
- Histórico de gráficos
- Serviços de recolha
- Inventário
- Utilizadores e grupo (excepto Enviar utilizador)
- Executar comando
- Instalar produtos
- Correcções (excepto Enviar correcções)

Tal como é mostrado na figura 4a abaixo, a aplicação Sincronizar data e hora estabelece ligações adicionais que não são mostradas na figura 4 acima. O servidor Java dos sistemas de destino na aplicação Sincronizar data e hora estabelece uma ligação ao servidor Java no sistema modelo, que por sua vez estabelece uma ligação ao servidor Java em cada sistema de destino.

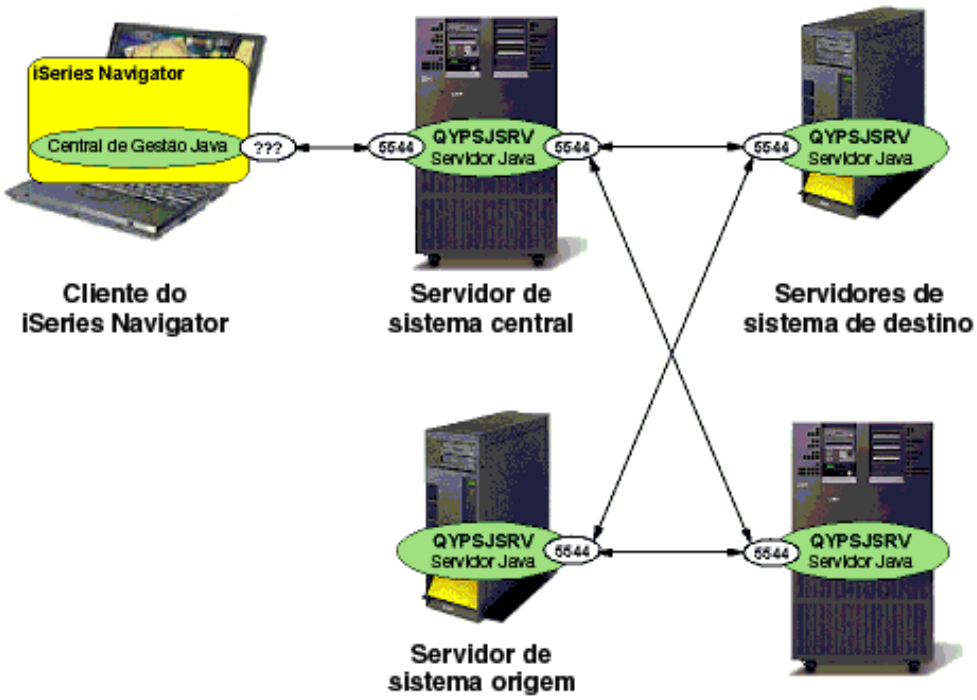

Figura 4a. Ligações para sincronizar data e hora para a Central de Gestão

Além disso, a aplicação Sincronizar funções trata o respectivo sistema modelo como outro destino final, o que significa que o servidor Java no CS contacta o servidor Java no sistema modelo e o servidor Java no sistema modelo contacta o servidor Java no CS.

Extensões Java

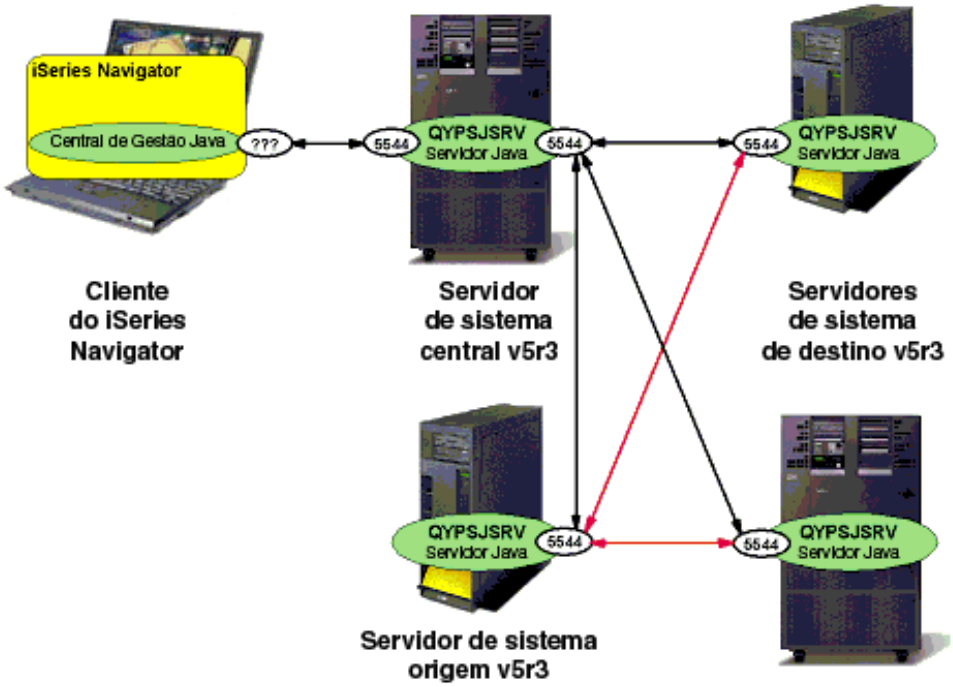

Figura 5. Ligações para extensões Java para a Central de Gestão (Ligações de BDT no Red)

A infra-estrutura em Java na V5R3 adicionou uma função de transferência de ficheiros [Transferência em massa de dados (BDT - Bulk Data Transfer)] entre um servidor origem e vários servidores de destino iSeries. Esta função BDT tem o mesmo objectivo que a função BDT em C++ (consulte a secção ″Extensões C++″ acima), embora esteja implementada de modo diferente. A função de transferência de ficheiros Java utiliza a porta da infra-estrutura em Java de modo a realizar a transferência de ficheiros, embora só esteja disponível entre sistemas origem e sistemas de destino V5R3 e posterior, uma vez que esta funcionalidade é nova na V5R3. Para realizar a transferência de ficheiros entre um sistema origem e um sistema de destino em que um (ou ambos) dos sistemas pertence à V5R2 ou anterior, é utilizada a função de transferência de ficheiros C++ e as portas associadas.

A Figura 5 acima mostra as ligações utilizadas para BDT Java entre um sistema origem e sistemas de destino V5R3. Note que quando utiliza um sistema origem e um sistema de destino V5R3, a Transferência em massa de dados utiliza ligações iniciadas na porta 5544, o que significa que o intervalo de números de portas mencionado na secção ″Extensões C++″ acima não está a ser utilizado. No entanto, se o sistema origem ou o sistema de destino pertencer a uma edição anterior à V5R3, é utilizado este intervalo de portas (uma vez que as portas de Extensões C++ estão a ser utilizadas).

A partir da V5R3, as seguintes aplicações da Central de Gestão utilizam a infra-estrutura em Java e optimizam também a funcionalidade de transferência de ficheiros Java.

- Distribuição de pacotes

- Enviar produtos
- Enviar utilizador
- Enviar correcções

Note que estas aplicações utilizam a funcionalidade de transferência de ficheiros Java apenas quando os sistemas V5R3 e posteriores estão envolvidos. As comunicações que incluem, pelo menos, um sistema V5R2 ou anterior continuam a utilizar a funcionalidade de transferência de ficheiros C++ (consulte a secção ″Extensões C++″ para obter detalhes).

Servidores do sistema central

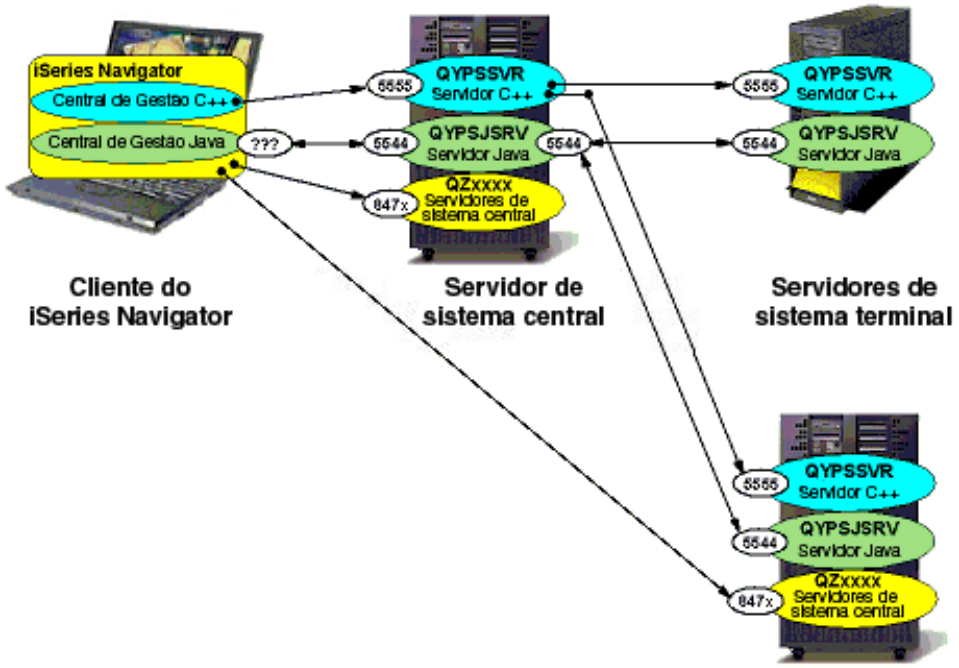

Figura 6. Ligações para servidores do sistema central utilizadas pela Central de Gestão

Num Cliente Gráfico do iSeries Navigator, as aplicações distribuídas da Central de Gestão estão associadas entre si a funções de sistema único do iSeries Navigator. Estas funções se sistema único do Navigator estabelecem ligações de terminal TCP/IP ponto a ponto a um conjunto de Servidores do sistema central iSeries. As ligações de terminal ponto a ponto a estes Servidores do sistema central iSeries são partilhadas entre aplicações em cada cliente do iSeries Navigator. Várias implementações da aplicação da Central de Gestão optimizam estas ligações partilhadas ao Servidor do Sistema Central no Cliente Gráfico para interagir com o Sistema Central. Do mesmo modo, poucas aplicações da Central de Gestão optimizam estas ligações para interagir directamente com Sistemas de Destino Final. Por exemplo, a aplicação Comparação e actualização dos valores do sistema contacta o Sistema Modelo directamente a partir do Cliente Gráfico do iSeries Navigator para obter os Valores do Sistema a partir do sistema modelo. Os URLs de informação:
http://publib.boulder.ibm.com/iseries/V5R3/ic2924/index.htm?info/rzaii/rzaiihstsvrbyfnctn.htm e
http://publib.boulder.ibm.com/iseries/V5R3/ic2924/index.htm?info/rzaii/rzaiicahstsvr.htm documentam os Servidores do Sistema Central iSeries e as funções que os mesmos fornecem às aplicações do cliente. Para obter uma lista dos números de portas utilizados por cada Servidor do Sistema Central iSeries, aceda ao URL: http://www-1.ibm.com/servers/eserver/iseries/access/caiixe1.htm e seleccione APAR

II12227. Os números de portas utilizados pelos Servidores do Sistema Central iSeries, normalmente optimizados pelo intervalo da Central de Gestão de 8470 a 8476 para ligações não SSL e de 9470 a 9476 para ligações SSL.

Secure Sockets Layer

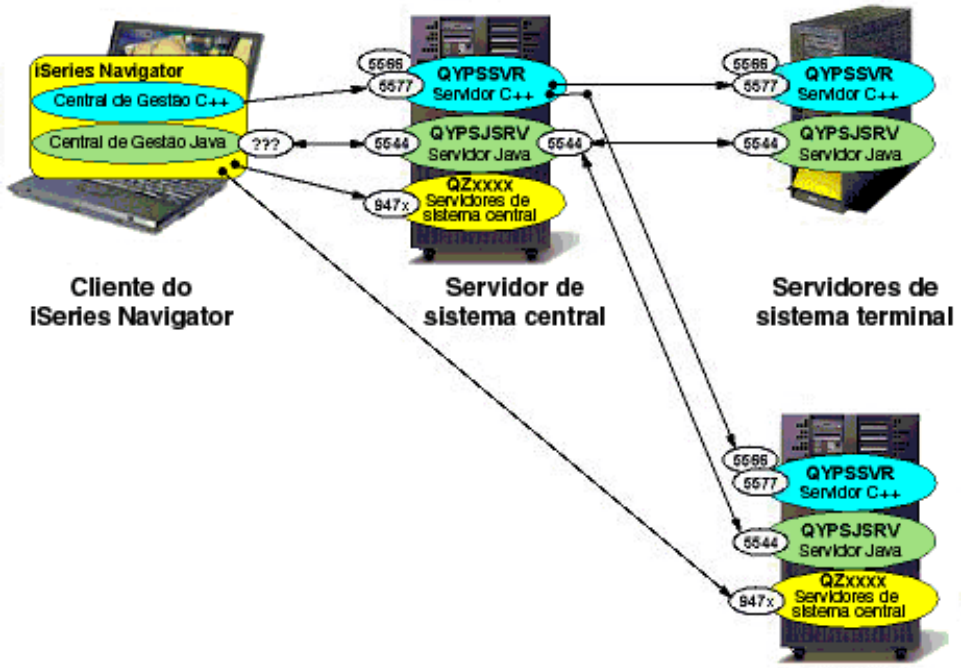

Figura 7. Ligações SSL da Central de Gestão

Se todos os Clientes Gráficos, Sistemas Centrais e Sistemas de Destino Final não estiverem na mesma rede local (por exemplo, se utilizar o Operations Navigator a partir de casa para gerir os sistemas iSeries no trabalho), o fluxo dos pedidos da Central de Gestão de sistemas e a partir dos mesmos é efectuado em redes fora do controlo do utilizador. Existe possibilidade de intercepção destes dados e a melhor forma de os proteger é utilizando SSL (Secure Sockets Layer). A Central de Gestão está activada para optimizar ligações SSL para fornecer segurança adicional através da encriptação de dados e validação de certificado. A configuração de SSL bem como da utilização do mesmo pela Central de Gestão num conjunto de servidores iSeries e de clientes do iSeries Navigator pode ser um desafio formidável.

O URL Centro de Informações da IBM:
http://publib.boulder.ibm.com/iseries/V5R3/ic2924/index.htm?info/rzain/rzainoverview.htm
documenta completamente a configuração de SSL para o iSeries Navigator e Central de Gestão [escolha as ligações “Plan for SSL enablement” (“Planear activação de SSL”) e, em seguida, “Secure applications with SSL -> Management Central” (“Proteger aplicações com SSL -> Central de Gestão”)]. Após a configuração da Central de Gestão para SSL e a activação de SSL, a Autenticação do servidor na infra-estrutura em C++ utilizará o número da porta 5566 e a Autenticação do servidor/cliente na infra-estrutura em C++ utilizará o número da porta 5577.

Quando o SSL está activado, o único impacto nas ligações e números de portas da Central de Gestão é que o número da porta 5555 na ligação da infra-estrutura em C++ acima é substituída por 5566 e/ou 5577, dependendo da autenticação seleccionada. A infra-estrutura em Java continua a utilizar o número da porta 5544, independentemente da activação de SSL ou da autenticação seleccionada. Cada um destes números de portas é configurável através das propriedades de configuração da Central de Gestão (Consulte a secção ″Configurações da ligação″).

Quando os Servidores do Sistema Central iSeries, normalmente optimizados pelas aplicações da Central de Gestão, são configurados para SSL, os números de portas utilizados por esses Servidores do Sistema Central variam entre 9470 e 9476.

Configurações da ligação

Várias características da ligação da Central de Gestão de cada Servidor e Cliente do iSeries Navigator são configuráveis. A seguinte tabela fornece uma lista de características da ligação da Central de Gestão com o mecanismo de configuração e valor/comportamento assumido.

Configuração do servidor com Entradas da tabela de assistência (Todas as edições) - WRKSRVTBLE

Característica da ligação	*Mecanismo de configuração*	*Valor assumido*
Porta do servidor Java	Serviço “as-mgtctrlj - Protocolo ″tcp“	5544
Porta não SSL do servidor C++ (utilizada pelo servidor Java na V5R3)	Serviço ″as-mgtctrl’ - Protocolo “tcp”	5555
Porta de validação do servidor C++ (utilizada pelo servidor Java na V5R3)	Serviço “as-mgtctrl-ss’ - Protocolo ″tcp“	5566
Porta de validação do Cliente/servidor SSL C++ (utilizada pelo servidor Java na V5R3)	Serviço ″as-mgtctrl-cs’ - Protocolo “tcp”	5577

Configuração do servidor com variáveis de ambiente ao nível do sistema (só V5R2)- WRKENVVAR LEVEL(*SYS)

Característica da ligação	*Mecanismo de configuração*	*Valor assumido*
Intervalo de portas da Transferência de ficheiros	Variável “QYPS_MINIMUM_PORT”	1024
Intervalo de portas da Transferência de ficheiros	Variável “QYPS_MAXIMUM_PORT”	32768

Configuração do servidor no ficheiro “/QIBM/UserData/OS400/MGTC/config/McConfig.properties” (só V5R1 e V5R2):

Característica da ligação	*Mecanismo de configuração*	*Valor assumido*
Nome do sistema central do servidor Java	Propriedade ″QYPS_HOSTNAME=xxxx″	Endereço de IP/Nome do sistema central

Configuração do servidor no ficheiro “/QIBM/UserData/OS400/MGTC/config/McEPConfig.properties” (só V5R3)

Característica da ligação	*Mecanismo de configuração*	*Valor assumido*
Intervalo de portas da Transferência de ficheiros	Propriedade ″QYPS_MINIMUM_PORT″	1024

Intervalo de portas da Transferência de ficheiros	Propriedade “QYPS_MAXIMUM_PORT”	32768
Nome do sistema central do servidor Java	Propriedade ″QYPS_HOSTNAME=xxxx	Endereço de IP/Nome do sistema central

Configuração do cliente no ficheiro (Todas as edições): C:\MgmtCtrl.properties

Característica da ligação	*Mecanismo de configuração*	*Valor assumido*
Nome do sistema central do cliente Java	Propriedade ″;QYPS_HOSTNAME=xxxx″	Endereço de IP/Nome do sistema central
Porta do cliente Java	Propriedade ″QYPSJ_LOCAL_PORT=xxxx″	aleatório

Nota: Os números de portas utilizados pelos Servidores do Sistema Central iSeries também podem ser configurados em cada servidor iSeries através das Entradas da tabela de assistência associadas.

Capítulo 3. Referência rápida da firewall da Central de Gestão

A secção que se segue fornece uma referência rápida para configurar a Central de Gestão para funcionar através de uma firewall. Este gráfico só é válido se a Central de Gestão e a configuração de rede estiverem configuradas do seguinte modo:

- As firewalls envolvidas não utilizam a Tradução do endereço de rede (NAT - Network Address Translation).
- QYPSJ_LOCAL_PORT=5544 está definida no ficheiro MgmtCtrl.properties do Cliente Gráfico. Para definir esta propriedade de modo a que a porta 5544 seja utilizada, crie um ficheiro de texto no PC em C:\MgmtCtrl.properties (se ainda não existir) e adicione a linha QYPSJ_LOCAL_PORT=5544
- A entrada da tabela de assistência as-mgtctrl está definida como 5555 (se o SSL estiver activado, a entrada as-mgtctrl-ss é 5566 e a entrada as-mgtctrl-cs é 5577) e a entrada as-mgtctrlj está definida como 5544 em todos os sistemas iSeries(TM). Estas são as definições assumidas, para verificar se foram alteradas utilize WRKSRVTBLE.

NOTA: Se o SSL estiver activado, será necessário abrir também as portas entre parêntesis

Tipo de aplicação	Aplicações	Portas a abrir na firewall do Cliente Gráfico	Portas a abrir na firewall do Sistema Central	Portas a abrir na firewall do Sistema Origem, se este for utilizado	Portas a abrir na firewall do Sistema de Destino Final
Infra-estrutura em Java(TM)	- Supervisor de trabalhos - Supervisor de mensagens - Supervisor de ficheiros - Supervisor de B2B - Tarefa BRMS - Sincronizar funções (utiliza o sistema origem)	5544	5544 5555 (5566, 5577) 8470 - 8476*	5544	5544
	- Movimentos agendados de recursos LPAR	5544	5544 5555 (5566, 5577) 8470 - 8476*	N/A	5544**
	- Sincronizar data e hora	5544	5544 5555 (5566, 5577) 8470 - 8476*	5544	5544
	- Comparação e actualização dos valores do sistema	5544	5544 5555 (5566, 5577) 8470 - 8476*	8470 - 8476*	5544

Infra-estrutura em C++ (Infra-estrutura em Java na V5R3)	- Supervisores do sistema - Histórico de gráficos - Serviços de recolha - Inventário - Utilizadores e grupos (excepto Enviar utilizador) - Executar comando - Instalar produtos - Correcções (excepto Instalar correcções)	N/A	5544 5555 (5566, 5577) 8470 - 8476*	N/A	5544 - só em sistemas V5R3 5555 (5566, 5577)
Extensões C++ (Extensões Java na V5R3)	- Distribuição de pacotes - Enviar produtos - Enviar utilizador - Enviar correcções	N/A	5544 5555 (5566, 5577) 8470 - 8476*	5544 - só em sistemas V5R3 5555 (5566, 5577)	5544 - só em sistemas V5R3 5555, (5566, 5577), intervalo de portas para o Cliente de transferência de ficheiros***

* 8470 - 8476 é o intervalo de portas que os servidores do sistema central utilizam. Cada aplicação da Central de Gestão utiliza um subconjunto diferente destas portas. Se estiver a utilizar o SSL para a Central de Gestão, deverá abrir as portas 9470 - 9476.

** Para os movimentos agendados de recursos LPAR, a partição primária é o único sistema de destino final.

*** Especificar QYPS_MINIMUM_PORT e QYPS_MAXIMUM_PORT:

- Para os sistemas de destino V5R2, é possível especificar as variáveis de ambiente QYPS_MINIMUM_PORT e QYPS_MAXIMUM_PORT ao nível do sistema em cada sistema de destino para definir o intervalo de portas utilizado pelo Cliente de transferência de ficheiros.
- Para os sistemas de destino V5R3, é possível especificar as variáveis de ambiente QYPS_MINIMUM_PORT e QYPS_MAXIMUM_PORT no ficheiro /QIBM/UserData/OS400/MGTC/config/McEPConfig.properties
- Para os sistemas de destino V5R1, este intervalo é 1024 - 32,768 e não pode ser alterado.

Consulte a secção ″Ligações da Central de Gestão″ para obter mais informações.

Capítulo 4. Limites da firewall da Central de Gestão devido à Tradução do Endereço de Rede

As firewalls, por definição, restringem os tipos de ligações que podem ser efectuadas para um determinado sistema ou conjunto de sistemas. Às vezes, de modo a que as aplicações distribuídas funcionem, a configuração da firewall e/ou configuração da aplicação necessitam de ser alteradas. Às vezes, não existem alterações na configuração que permitam que a aplicação funcione (excepto se desactivar ou remover completamente a firewall). Esta secção aborda as firewalls que utilizam a Tradução do Endereço de Rede (NAT - Network Address Translation) e as restrições que podem originar em aplicações distribuídas como, por exemplo, as aplicações da Central de Gestão.

Tradução do Endereço de Rede (NAT)

Muitas firewalls podem ser configuradas para utilizar a Tradução do Endereço de Rede (NAT - Network Address Translation). Para efectuar este procedimento, um administrador configura as regras onde alguns ou todos os pedidos recebidos e enviados dos sistemas protegidos têm o endereço de IP alterado para onde são enviados e de onde saem. Existem muitos tipos de Tradução do Endereço de Rede mas existem duas categorias principais: NAT dinâmico e NAT estático. Como regra geral (com algumas excepções), a maior parte das aplicações da Central de Gestão podem ser configuradas para funcionar com o NAT estático mas não podem ser configuradas para funcionar como NAT dinâmico.

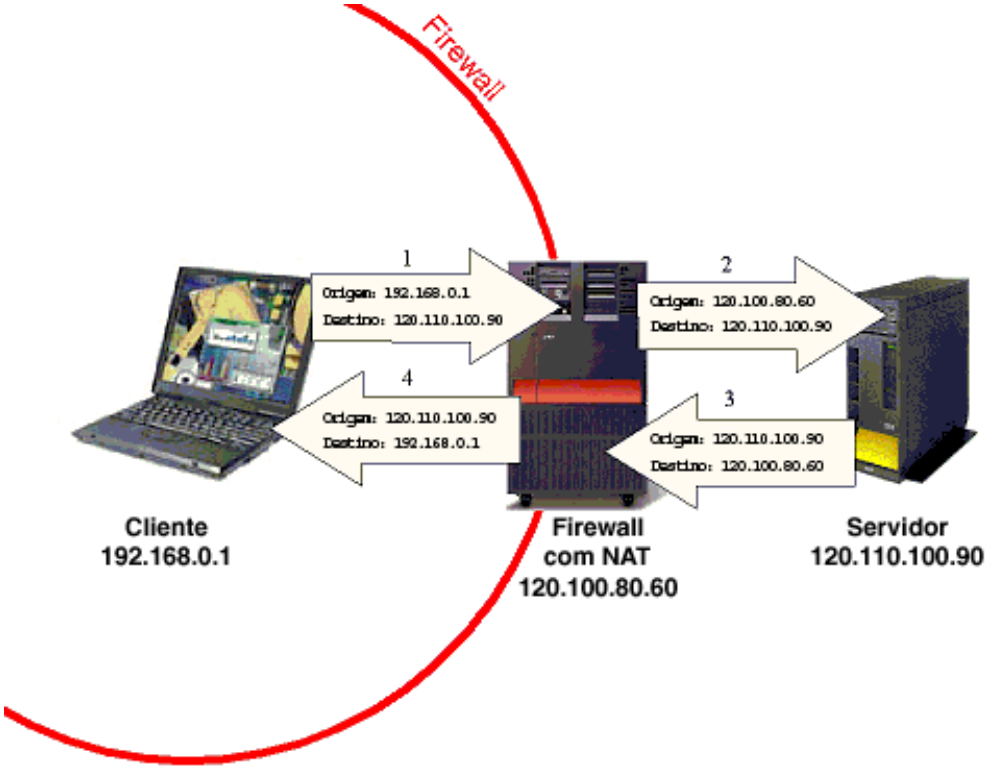

Figura 8. Tradução do Endereço de Rede

A situação onde o NAT pode ser utilizado está ilustrada acima. Quando um sistema com a firewall inicia uma ligação com um sistema fora da firewall (passo 1 no diagrama acima), a firewall aceita o pedido e substitui o endereço de IP de origem do pacote (o endereço de IP de onde vem o pacote) pelo endereço de IP externo da firewall (2). Desta forma, qualquer resposta relacionada com este pedido será enviada

para a firewall. Quando a resposta for enviada na mesma ligação (3), dirige-se à firewall (uma vez que no pedido de saída a firewall substituiu o endereço de IP de origem pelo endereço externo da firewall). A firewall recebe esta resposta, verifica se é uma resposta que deve ser permitida e remete-a (4) para o sistema interno correcto (alterando o endereço de IP de destino).

Tal como é apresentado acima, desde que o sistema interno inicie a ligação, o sistema fora da firewall pode comunicar com o sistema interno utilizando essa ligação. Isto acontece para o NAT estático e para o NAT dinâmico. A diferença entre o NAT estático e o dinâmico é a de que o NAT estático faz com que os sistemas externos consigam iniciar as ligações com sistemas dentro da firewall, o que não acontece com o NAT dinâmico.

NAT estático

O NAT estático tem uma tabela que faz a correspondência entre os endereço de IP internos e os endereços de IP externos. Se foi enviado um pedido de um sistema dentro da firewall com o endereço de IP interno 192.168.0.1, a firewall procura esse endereço interno na tabela para saber o endereço externo que deve ser utilizado para substituí-lo. Em seguida, quando a resposta é enviada a esse endereço de IP externo, a firewall utiliza novamente essa tabela para verificar o sistema interno que está associado a esse IP externo. Esta tabela é estática (o que significa que um endereço de IP externo do sistema interno será sempre o mesmo). Isto significa que os sistemas fora da firewall conseguem iniciar uma ligação a esse sistema interno desde que esse sistema externo conheça o endereço de IP externo do sistema interno.

NAT dinâmico

Com o NAT dinâmico, a firewall determina dinamicamente o endereço de IP externo a atribuir a um pedido de saída. Poderia acontecer que todos os pedidos obtivessem o mesmo endereço de IP externo ou obtivessem o endereço seguinte disponível numa área de endereços de IP externos. Uma vez que não existe uma tabela estática, numa determinada altura o sistema interno poderia ter o endereço externo 120.110.100.95 e numa altura posterior poderia ter o endereço externo 120.110.90.85. Sempre que a firewall substitui um endereço de IP interno por um endereço externo, efectua um registo deste procedimento de modo a que quando for enviada uma resposta na mesma ligação, a firewall consiga encaminhá-la para o endereço de IP interno correcto.

Esta forma de distribuição de endereços de IP externos faz com que os sistemas fora da firewall não consigam iniciar uma ligação a um sistema interno, (uma vez que o sistema externo não pode determinar o endereço de IP externo a utilizar). A única forma de um sistema fora da firewall poder comunicar com um sistema dentro da mesma é responder a um pedido iniciado pelo sistema dentro da firewall.

Limites da Central de Gestão

Todas as aplicações distribuídas (incluindo as aplicações da Central de Gestão) que necessitem de iniciar uma ligação a partir de um sistema externo para um sistema dentro de uma firewall não funcionarão com o NAT dinâmico. Para obter informações sobre como utilizar a Central de Gestão com uma instalação específica do NAT dinâmico, consulte a secção anterior ″Ligações da Central de Gestão″ para determinar as ligações que as aplicações da Central de Gestão utilizam (PC a CS, CS a PC, CS a EP, EP a CS, etc). Utilize essas informações juntamente com as informações sobre os sistemas e ligações que estão a utilizar o NAT dinâmico para descobrir as aplicações que irão funcionar ou não..

As aplicações distribuídas (incluindo as aplicações da Central de Gestão) que necessitam de estabelecer uma ligação a partir de um sistema externo para um sistema com uma firewall devem funcionar com o NAT estático. No entanto, muitas vezes estas aplicações têm de ser configuradas de modo a que o sistema externo que tenta estabelecer uma ligação ao sistema com a firewall utilize o endereço de IP externo desse sistema interno. Para a Central de Gestão, se um sistema (iSeries(TM) ou PC) tiver uma firewall que esteja a utilizar o NAT estático, esse sistema necessita de definir a respectiva propriedade

QYPS_HOSTNAME para o endereço de IP externo. Ou, se esse sistema tiver sistemas dentro e fora da firewall aos quais estabelece ligação, necessitará de definir a respectiva propriedade QYPS_HOSTNAME para um nome do sistema central que irá processar para o respectivo endereço de IP interno em sistemas internos e para o respectivo endereço de IP externo em sistemas externos. A secção ″Ligações da Central de Gestão″ descreve a forma como definir esta propriedade QYPS_HOSTNAME (definir esta propriedade difere de acordo com a edição do sistema).

Capítulo 5. Cliente Gráfico protegido por uma firewall

Os Clientes Gráficos da Central de Gestão, que também são utilizados para estabelecer ligação directamente à Internet, estão muitas vezes protegidos por uma firewall. A utilização de firewalls de software e/ou de hardware com acesso de velocidade rápida à Internet em residências está a tornar-se muito comum. Sem uma configuração especial necessária, este ambiente de firewall simples pode restringir a funcionalidade da Central de Gestão.

Objectivos

Configuração detalhada da Central de Gestão necessária num ambiente de firewall comum em que o Cliente Gráfico está protegido por uma firewall.

Detalhes

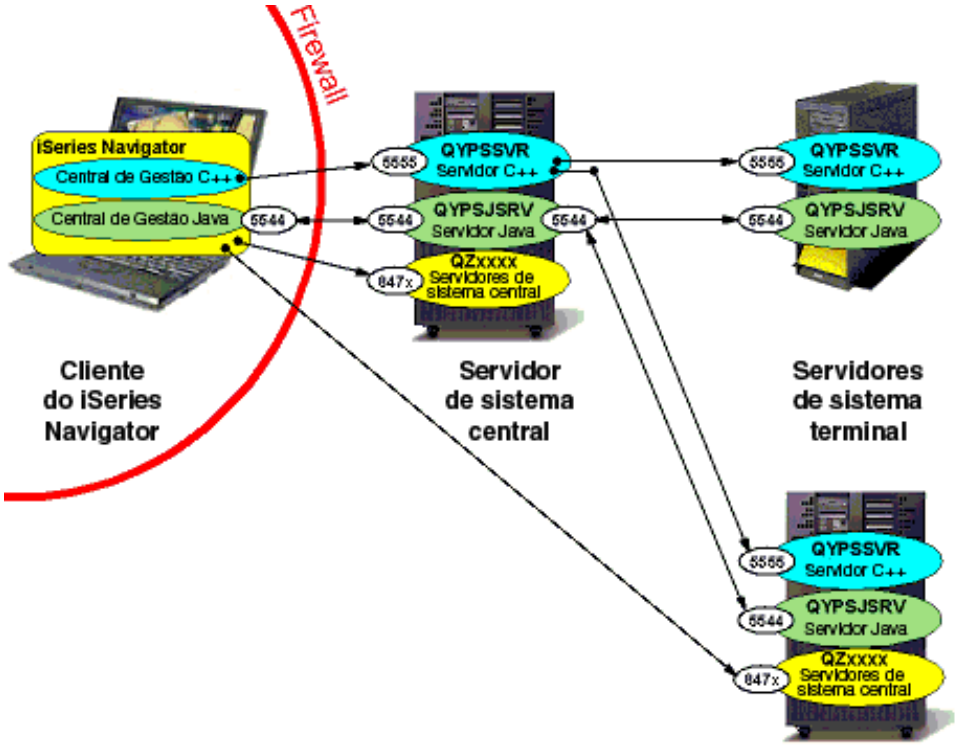

Figura 9. Cliente Gráfico protegido por uma firewall

Eis alguns pontos importantes a ter em consideração sobre o diagrama acima:

- As comunicações entre o Sistema Central e o Sistema de Destino Final não são afectadas, uma vez que se realizam fora da firewall. Se existiam firewalls adicionais entre o Sistema Central e os Destinos finais, consulte o cenário três ou consulte a secção "Ligações da Central de Gestão" para obter informações sobre a configuração dessas ligações.
- Neste diagrama, é apresentado o servidor C++, embora em sistemas v5r3 o servidor C++ não exista e o servidor Java efectue recepções na porta 5555

- As ligações do Cliente Gráfico ao servidor C++ da Central de Gestão na porta 5555 (ou servidor Java na v5r3) e ao servidor Java(TM) na porta 5544 no Sistema Central do iSeries(TM) podem estabelecer ligações através da firewall sem configuração adicional nas portas 5544 e 5555.
- As ligações do Cliente Gráfico aos servidores do Sistema Central no Sistema Central do iSeries podem estabelecer ligações através da firewall sem configuração adicional.
- Como valor assumido, é seleccionada uma porta aleatória para a ligação do servidor Java no Sistema Central ao Cliente Gráfico. Para este cenário, é necessário definir uma única porta no ficheiro de propriedades do PC da Central de Gestão (consulte a secção ″Configurações da ligação″) de modo a que não seja utilizada uma porta aleatória para estabelecer ligação entre o Sistema Central e o Cliente Gráfico (no diagrama, foi seleccionada a porta 5544, embora seja possível utilizar outra). Consulte as instruções abaixo para obter mais informações sobre este assunto.
- Se estiver a utilizar o SSL, será necessário incluir as portas 5566 e 5577 com a 5555 ao longo deste documento.

Os passos para configurar a Central de Gestão são ligeiramente diferentes, dependendo do modo como a firewall está configurada para utilizar NAT.

Warning: Temporary Level 2 Header

Firewall que não esteja a utilizar NAT

- Defina a porta utilizada para estabelecer ligação a partir da Central de Gestão ao Cliente Gráfico como uma porta específica, conforme é descrito no ponto de destaque quatro acima e conforme é ilustrado no diagrama (consulte a secção ″Ligações da Central de Gestão″ para obter detalhes).
- Configure a firewall para abrir a porta específica de modo a que o tráfego a partir do Sistema Central possa chegar ao Cliente Gráfico.

Firewall que utiliza NAT estático

- Siga as instruções (acima) para uma firewall que não esteja a utilizar NAT.
- Defina a propriedade QYPS_HOSTNAME no Cliente Gráfico (consulte a secção ″Ligações da Central de Gestão″) como o endereço de IP externo deste Cliente Gráfico (o endereço de IP utilizado por sistemas fora da firewall para contactar com este Cliente Gráfico).

Firewall que utiliza NAT dinâmico

Se a firewall que protege o Cliente Gráfico estiver a utilizar NAT dinâmico, o Sistema Central não poderá contactar novamente com o Cliente Gráfico. Isto impedirá o funcionamento de todas as aplicações da Central de Gestão que utilizam a infra-estrutura em Java. As aplicações que não utilizam a infra-estrutura em Java (incluindo as aplicações que eram C++ na V5R2 e que foram convertidas para aplicações Java na V5R3) funcionam perfeitamente sem ser necessária qualquer configuração (uma vez que é apenas a infra-estrutura em Java que estabelece novamente ligação ao PC).

Capítulo 6. Sistema Central protegido por uma firewall

As firewalls de software e/ou de hardware que protegem a rede interna de uma empresa do tráfego da Internet constituem outro ambiente de firewall comum. Quando o Cliente Gráfico, que está a tentar estabelecer ligação ao Sistema Central da Central de Gestão, está localizado fora da firewall, é necessária configuração de modo a permitir a funcionalidade completa da Central de Gestão.

Objectivos

Configuração detalhada da Central de Gestão necessária num ambiente de firewall comum em que os servidores do Sistema Central e do Sistema de Destino Final iSeries(TM) estão protegidos por uma firewall e o Cliente Gráfico está fora dessa firewall.

Detalhes

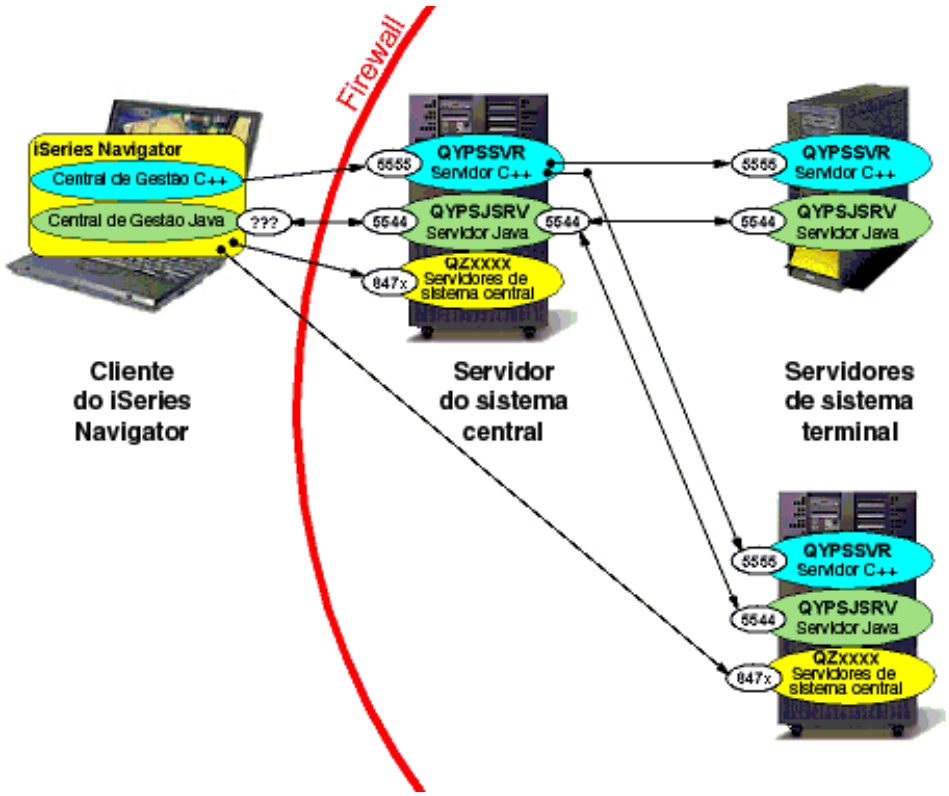

Figura 10. Sistemas iSeries (Sistema Central e Sistema de Destino Final) protegidos por uma firewall

Eis alguns pontos importantes a ter em consideração sobre o diagrama acima:

- As comunicações entre o Sistema Central e o Sistema de Destino Final não são afectadas, uma vez que se realizam dentro da firewall. Se existiam firewalls adicionais entre o Sistema Central e os Destinos finais, consulte o cenário três ou consulte a secção "Ligações da Central de Gestão" para obter informações sobre a configuração dessas ligações.
- Neste diagrama, é apresentado o servidor C++, embora em sistemas V5R3 o servidor C++ não exista e o servidor Java efectue recepções na porta 5555

- O Cliente Gráfico irá necessitar de estabelecer ligação ao servidor C++ da Central de Gestão na porta 5555 (ou ao servidor Java na v5r3) e ao servidor Java(TM) porta 5544 no Sistema Central iSeries.
- O Cliente Gráfico irá necessitar de estabelecer ligação a alguns servidores do sistema central no Sistema Central, e possivelmente a outros sistemas (por exemplo, o Cliente Gráfico contacta o sistema modelo directamente utilizando o servidor do sistema central para a aplicação Comparação e actualização dos valores do sistema).
- Se estiver a utilizar o SSL, será necessário incluir as portas 5566 e 5577 com a 5555 ao longo deste documento.

Os passos para configurar a Central de Gestão são ligeiramente diferentes, dependendo do modo como a firewall está configurada para utilizar NAT.

Firewall que não esteja a utilizar NAT

- Abra as portas 5544 e 5555 na firewall de modo a que o Cliente Gráfico possa estabelecer ligação ao Sistema Central da Central de Gestão.
- Abra as portas do servidor do sistema central na firewall necessárias às funções da Central de Gestão que estão a ser utilizadas. Para obter informações gerais adicionais sobre a configuração de servidores do sistema central para funcionarem através de uma firewall, aceda a http://www-1.ibm.com/servers/eserver/iseries/access/cafirewl.htm

Firewall que utiliza NAT estático

- Siga as instruções (acima) para uma firewall que não esteja a utilizar NAT.
- Defina o Sistema Central no iSeries Navigator para estabelecer ligação ao endereço de IP externo do Sistema Central (certificando-se de que o Sistema Cem My Connections (As minhas ligações) está a utilizar o endereço de IP externo).
- Defina QYPS_HOSTNAME no Sistema Central conforme descrito na secção ″Ligação da Central de Gestão″. Existem duas formas para executar esta operação:
  1. Defina QYPS_HOSTNAME do Sistema Central como o endereço de IP externo do Sistema Central. Isto significa que qualquer sistema da Central de Gestão (incluindo os Sistemas de Destino Final, que poderão estar localizados dentro da firewall) irá estabelecer ligação ao Sistema Central utilizando o endereço de IP externo.
  2. Defina QYPS_HOSTNAME como um determinado nome do sistema central que irá resolver o endereço de IP externo do Sistema Central em sistemas externos (por exemplo, o Cliente Gráfico) e também em sistemas internos.

Firewall que utiliza NAT dinâmico

Se a firewall que protege o Sistema Central estiver a utilizar NAT dinâmico, o Cliente Gráfico não poderá contactar com o mesmo. De facto, nenhum sistema fora da firewall poderá iniciar uma ligação ao Sistema Central para utilizar qualquer aplicação distribuída.

Capítulo 7. Sistemas de Destino Final protegidos por uma firewall

Em determinadas situações, poderá pretender utilizar um Sistema Central numa localização física para gerir um conjunto de Sistemas de Destino Final noutra localização. Neste caso, esses sistemas de destino final estarão provavelmente protegidos por uma firewall, pelo que poderão ocorrer alguns problemas nesta situação. Este cenário explicará os problemas que poderão surgir e explica como corrigi-los.

Objectivos

Explicar a configuração da Central de Gestão necessária num ambiente de firewall em que os Sistemas de Destino Final estão protegidos por uma firewall e ambos o Cliente Gráfico e o Sistema Central estão localizados fora dessa firewall.

Detalhes

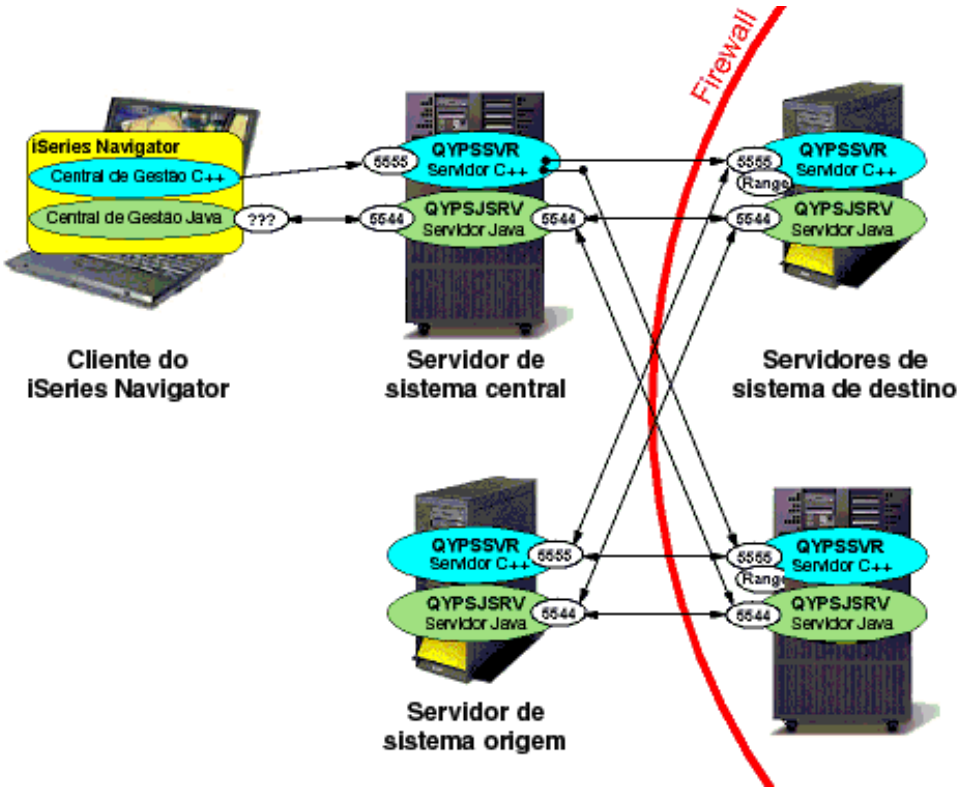

Figura 11. Sistemas de Destino Final protegidos por uma firewall

Este diagrama mostra as ligações que é necessário estabelecer através da firewall que protege os Sistemas de Festino Final. Eis alguns pontos importantes a ter em consideração no diagrama acima:

- Este diagrama assume que a ligação do Cliente Gráfico ao Sistema Central não está a ser estabelecida através de uma firewall. Se não for este o caso, consulte os cenário um e dois ou consulte a secção "Ligações da Central de Gestão" para obter informações sobre como configurar a ligação.
- Neste diagrama é apresentado o servidor C++, embora em sistemas V5R3 o servidor C++ não exista e o servidor Java efectue recepções na porta 5555.

- Este diagrama não inclui as ligações do servidor do sistema central estabelecidas a partir do Cliente Gráfico ao Sistema Central ou a partir do Cliente Gráfico aos Sistemas de Destino Final. É importante que a firewall esteja configurada para permitir estas ligações. Consulte o cenário 2 para obter informações sobre o que é necessário fazer de modo a permitir estas ligações.
- Neste diagrama o sistema origem encontra-se localizado fora da firewall (pode ser o Sistema Central ou outro sistema fora da firewall). Se o sistema origem estiver localizado dentro da firewall, não ocorrerão quaisquer problemas de ligação (uma vez que os sistemas de destino final com os quais o sistema origem comunica também se encontram localizados dentro da firewall), pelo que não será necessária a configuração completa descrita abaixo.
- O CS comunicará com os Sistemas de Destino Final em duas portas, a 5544 e a 5555
- Se estiver a utilizar o SSL, será necessário incluir as portas 5566 e 5577 com a 5555 ao longo deste documento.
- Note no diagrama que, se uma aplicação utilizar BDT (uma extensão C++), cada sistema de destino (destino final) seleccionará uma porta aleatória para efectuar a recepção e o servidor BDT do sistema modelo/origem contactará o sistema de destino final nessa porta para transferir os dados.
- Para os sistemas de destino final V5R2 e V5R3, é possível especificar um intervalo de portas para esta porta BDT utilizando as propriedades QYPS_MINIMUM_PORT e QYPS_MAXIMUM_PORT descritas na secção "Ligações da Central de Gestão". Cada tarefa em execução necessita de uma porta BDT separada durante o respectivo arranque pelo que, se tiver 7 aplicações da Central de Gestão que utilizam BDT com arranque no mesmo sistema de destino ao mesmo tempo, o intervalo terá de ter, pelo menos, 7 portas.

Os passos para configurar a Central de Gestão são ligeiramente diferentes, dependendo do modo como a firewall está configurada para utilizar NAT.

Firewall que não esteja a utilizar NAT

Se a firewall não utilizar a Tradução do endereço de rede (NAT - Network Address Translation), a configuração será bastante simples

- Abra as portas 5544 e 5555 na firewall, de modo a que o Sistema Central e o Sistema Origem possam estabelecer ligação aos Sistemas de Destino Final.
- Consulte o cenário 2 para obter informações sobre a permissão de ligações do servidor do sistema central.
- Especifique um intervalo de portas em cada um dos sistemas de destino suficientemente grande de modo a ter uma porta para todas as aplicações BDT com arranque ao mesmo tempo.
- Abra este intervalo de portas na firewall de modo a que o sistema modelo/origem possa enviar dados aos sistemas de destino.

Firewall que utiliza NAT estático

- Siga as instruções (acima) para uma firewall que não esteja a utilizar NAT.
- Certifique-se de que cada Sistema de Destino Final na Central de Gestão protegido pela firewall tem o respectivo endereço de IP externo especificado na lista de sistemas de destino final no Sistema Central (uma vez que o Sistema Central não poderá estabelecer ligação ao endereço de IP externo para qualquer sistema de destino final). Ou, se a frequência de consulta estiver definida como sempre, certifique-se de que no Sistema Central os nomes dos sistemas de destino final resolvem o endereço de IP externo desses sistemas de destino final.
- Defina QYPS_HOSTNAME em cada Sistema de Destino Final, conforme descrito na secção "Ligações da Central de Gestão". É definido numa das duas seguintes formas:
  1. Defina QYPS_HOSTNAME como o endereço de IP externo nesse sistema. Isto significa que qualquer sistema da Central de Gestão (incluindo um sistema modelo dentro da firewall), irá estabelecer ligação ao Sistema Central utilizando o endereço de IP externo.

2. Defina QYPS_HOSTNAME como um determinado nome do sistema central que resolverá o endereço de IP externo desse Sistema de Destino Final em sistemas externos (por exemplo, o Sistema Central) e também em sistemas internos.

   NOTA: A definição de QYPS_HOSTNAME como um nome do sistema central (em oposição a um endereço de IP) funcionará bem para as extensões e infra-estrutura em Java(TM), que transmitem este valor QYPS_HOSTNAME para a resolução de outros sistemas. No entanto, a definição de QYPS_HOSTNAME como um nome do sistema central em oposição a um endereço de IP externo não afectará a extensão C++ [Transferência em massa de dados (BDT - Bulk Dtaa Transfer)]. Se QYPS_HOSTNAME estiver realmente definido como o nome do sistema central e não um endereço de IP, o cliente de Transferência em massa de dados em cada Sistema de Destino Final resolverá este QYPS_HOSTNAME para um endereço de IP utilizando primeiro a tabela do sistema central ou DNS nesse sistema de destino final e, em seguida, transmitindo o nome do sistema central a um sistema remoto para que seja resolvido aí). Por último, a infra-estrutura em C++ não utiliza este valor QYPS_HOSTNAME, de modo que não surgirão quaisquer tipos de problema.

Firewall que utiliza NAT dinâmico

Se a firewall que protege os Sistemas de Destino Final estiver a utilizar NAT dinâmico, o Sistema Central não poderá contactar com os mesmos. De facto, nenhum sistema fora da firewall poderá iniciar uma ligação a nenhum Sistema de Destino Final para utilizar qualquer aplicação distribuída.